2013-12

A feasibility study of implementing a bring-your-own-computing-device policy

Carideo, Jeffrey W.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

A FEASIBILITY STUDY OF IMPLEMENTING A BRING-YOUR-OWN-COMPUTING-DEVICE POLICY

By: **Jeffrey W. Carideo,**
Timothy P. Walker,
Jason C. Williams

December 2013

Advisors: **Douglas E. Brinkley**
Steven P. Landry

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** MBA Professional Report	
4. TITLE AND SUBTITLE A FEASIBILITY STUDY OF IMPLEMENTING A BRING-YOUR-OWN-COMPUTING-DEVICE POLICY		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jeffrey W. Carideo, Timothy P. Walker, Jason C. Williams			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER** N/A	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Our team conducted an information technology study on the feasibility of reduction of hardware and software procurement expenditures at the Naval Postgraduate School, Graduate School of Business and Public Policy (GSBPP). The objectives were to calculate the total cost of the GSBPP's current expenditures, develop alternative hardware and software procurement plans, and measure these costs against the alternative plan of implementing a bring-your-own-device policy for economic, operational, and technical feasibility.

14. SUBJECT TERMS: Bring-your-own device (BYOD), hardware and software procurement plans, cost analysis, cloud computing, simplified structures, management server licensing	**15. NUMBER OF PAGES** 95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A FEASIBILITY STUDY OF IMPLEMENTING A BRING-YOUR-OWN-COMPUTING-DEVICE POLICY

Jeffrey W. Carideo, Lieutenant, United States Navy
Timothy P. Walker, Lieutenant, United States Navy
Jason C. Williams, Lieutenant, United States Navy

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Authors:

_____
Jeffrey W. Carideo

_____
Timothy P. Walker

_____
Jason C. Williams

Approved by:

_____
Douglas E. Brinkley, PhD

_____
Steven P. Landry, PhD

_____
William R. Gates, PhD
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

A FEASIBILITY STUDY OF IMPLEMENTING A BRING-YOUR-OWN-COMPUTING-DEVICE POLICY

ABSTRACT

Our team conducted an information technology study on the feasibility of reduction of hardware and software procurement expenditures at the Naval Postgraduate School, Graduate School of Business and Public Policy (GSBPP). The objectives were to calculate the total cost of the GSBPP's current expenditures, develop alternative hardware and software procurement plans, and measure these costs against the alternative plan of implementing a bring-your-own-device policy for economic, operational, and technical feasibility.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AE	academic edition
BYOC	bring your own computer
BYOD	bring your own device
CA	cost analysis
CAL	client access license
CENIC	Corporation for Educational Network Initiatives in California
CBLSA	Crystal Ball License Service Agreement
CIO	chief information officer
COA	course of action
DMTF	Distributed Management Task Force
ECAR	EDUCAUSE Center for Applied Research
EULA	end-user license agreement
FAST	Federation against Software Theft
GSBPP	Graduate School of Business and Public Policy
HPC	high performance computing
HPR	high performance research
IaaS	infrastructure as a service
ISV	independent software vendor
IT	information technology
LCC	Lansing Community College
LSS	license server software
MBA	Master of Business Administration
ML	management license
NPS	Naval Postgraduate School
NVCC	Northern Virginia Community College
OSE	operating system environments
PaaS	platform as a service
PC	personal computer
PGCC	Prince George Community College

SaaS	software as a service
SOW	statement of work
VDI	virtual desktop infrastructure

ACKNOWLEDGMENTS

The members of the research team collectively wish to thank our academic advisors at the Naval Postgraduate School. In particular, we wish to thank Dr. Douglas Brinkley, who introduced us to the project. We would also like to thank Dr. Steven Landry for his mentorship throughout our tenure at NPS. Without their support and mentorship, this project would not have been possible.

Individually, we wish to thank our families for their tireless support and patience while we worked on this project. Most important of all, we give thanks to God for the multitude of blessings in our lives.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A subjective and un-scientific analysis of the Graduate School of Business and Public Policy's (GSBPP's) current program for providing laptops for student use during certain classes led to the idea that the school may find cost savings by asking each student to bring his or her own computing device to school. In this paper, we evaluate the technical issues, the legal difficulties, and the potential costs of implementing a bring-your-own-device (BYOD) policy in the business school.

There are situations where faculty members determine that it is necessary to have students use special software to meet class objectives; however, these situations appear to be infrequent and are out of balance with the amount of school-provided hardware available in the classrooms. We believe that there are potential cost savings that can be realized on the hardware the school purchases. We envision that each student will bring his or her own laptop to the classroom when required. We make the assumption that most students have a personal laptop; however, consideration is given to the utilization of a loaner program for those who do not.

The foundation for addressing the most cost-effective and beneficial end-state for the business school is developed through a cost analysis. We collect software usage data utilized by the business school's faculty and staff regarding technology use in the classroom. Essential software is then tested through applied and technical application utilizing a client server to determine whether software can run without limitations, while ensuring legal compliance with the software's restriction policy. In identifying essential software requirements for the GSBPP, the analysis also helps us to determine whether there are any software reduction requirements or impact to both staff and students due to reduced classroom hardware.

A. PURPOSE

The purpose of this MBA project is to determine the best alternative based on the most cost-efficient course of action. This analysis is accomplished using unbiased quantitative data and analysis. All alternatives are compared, including the option of

doing nothing. We address and answer whether the benefits of a BYOD program outweigh current costs, and whether BYOD benefits the GSBPP without compromising its academic structure.

B. RESEARCH QUESTIONS

This MBA project evaluates whether it would be technically and economically feasible for the GSBPP to adopt a BYOD policy and require students to use their own laptops. The method of providing software to the student computers would incorporate client–server architecture. The research addresses the following topics:

1. Technical issues—Is all of the software used in the GSBPP curricula compatible with a client–server architecture? Is the campus network infrastructure reliable enough to support client–server architecture?
2. Cost analysis—What would be the return on investment in adapting the new business model? Some computers will be kept on campus for computer labs and to support students who cannot afford to buy their own laptops. The cost analysis includes sensitivity analysis to determine how the return on investment is affected by varying numbers of government-owned machines left under the old business model.
3. Legal issues—Do all of the GSBPP software licenses permit operation under client–server architecture?
4. How might the GSBPP at NPS apply lessons learned from other educational institutions in the implementation of a BYOD policy?

C. BACKGROUND

The GSBPP maintains approximately 144 government-owned laptops in four so-called smart classrooms for use by approximately 325 resident students. The computers are purchased by the GSBPP and maintained by two computer technicians with funds budgeted and provided through NPS. The hypothesis of our research team is that these computers are underutilized and that most students are more comfortable using their own laptops and other computing devices, which they bring to NPS with them each day. Additionally, as furloughs and sequestration are an everyday topic of concern at NPS, potential areas for budget cuts and general means of executing fiduciary responsibility should be examined at every opportunity.

Currently, the GSBPP budgets $50,000 per year for hardware refreshes of laptops that have reached the end of their three-year cycle, with approximately 36 computers purchased each year. Each computer costs approximately $1,300 for hardware, dependent on market conditions and contract terms and conditions of each given purchase. An additional $10,000 per year is spent on licensing software peculiar to the GSBPP. The GSBPP also allocates approximately $20,000 per year for hardware and software dedicated to an application server that delivers some software to students in a client–server architecture (D. Brinkley, interview with author, September 17, 2013).

D. RESEARCH SETTING

A BYOD policy would greatly reduce, or possibly eliminate, the cost of laptop hardware refreshes, but software costs, server costs, and computer technical support staff salaries remain as a concern to be addressed. All software used for classes and assignments would be pushed to a "cloud" atmosphere or a thin-client/server architecture.

Preliminary research has shown that many other educational institutions, from the high school level to the graduate school level, have minimized their computing costs by making students provide their own laptops. Our research determines whether such a course of action is feasible for the GSBPP.

E. ORGANIZATION OF STUDY

This report describes the feasibility of requiring students at NPS to bring their own computing devices and whether the benefits of the program outweigh the current costs without compromising the academic structure. In Chapter II, we present a literature review on the academic concepts used to compose the research framework. In Chapter III, we explain the methods used for this study. Chapter IV details this study's analysis and findings. In Chapter V, we discuss pertinent discoveries and implications and give recommendations to address those discoveries. In Chapter VI, we detail final thoughts, limitations of the research, recommendations for further research, and the overall benefits of the study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. TECHNICAL ISSUES

A thin-client/server architecture and BYOD models are still relevant even in the age of cloud computing. Such models allow the end users, in our case students, to access software and applications from multiple locations using various personal devices. The GSBPP must determine whether the thin-client and BYOD model will meet its needs in the academic environment. There are advantages to using a thin-client server, which include reliability and lower operating cost. Essentially, time savings occur because technicians no longer must install software on individual computing devices. Only the thin-client/server architecture requires updates and management.

Thin-clients also provide a smaller surface area for security threats. Should users become infected with a virus, we can simply have them log off and log back in. They will be logged into a new and healthy virtual desktop. Further, if a device is stolen, there would be no loss of data because there is no data on the device. Finally, due to the smaller hardware footprint and sometimes no moving parts, the lifespan of a thin client is five to seven years compared to a normal three-year life span (Myer, 2013).

However, disadvantages to the thin-client/server architecture include client limitations and a single point of failure, which can disrupt a student's ability to use software applications needed to complete academic work if the server ever goes down or if there are any network disconnections. One "concern operating in a BYOD environment is finding a secure and effective way to deploy applications and software to various devices while meeting the organization's security framework" (Myer, 2013). It is imperative for the GSBPP to meet the standards as prescribed by the Department of Defense. Once that is achieved, best practices must be identified, for instance, choosing one manufacturer of devices across the GSBPP and training faculty, students, instructors, and staff on proper use of the system. Planned contingencies should be in place to help minimize any downtime that could affect the GSBPP academic environment.

B. COST ANALYSIS

The model for a BYOD program for education closely follows a corporate trend where companies have initiated mandatory BYOD policies or allowed their employees to participate voluntarily in such programs. We have found an array of reports from various companies and educational institutions that outline expectations of cost, anticipated cost savings, and an analysis of what cost savings, expenses, and benefits are actually present at the onset and into the maturity of a BYOD program.

Paul Ardoin, Director of North American Marketing for cloud services provider VisionApp, wrote a white paper in March 2010 in which he forecasted the next decade as "the decade of Bring Your Own Computer (BYOC)," a term that is often used interchangeably with BYOD. He concentrated on Cintrix corporation's lauded efforts to introduce a BYOC program in 2009. Ardoin astutely stated that although companies often see heavy upfront costs as they invest in networking services, they generally see an overall decline in expenses (2010):

> As with any major project, this can require a significant up-front investment, but visionapp has seen that the return on that investment can be recaptured quickly. One enterprise client invested more than $10 million up front, but they saved almost $50 million in IT operations costs over the first 36 months–well beyond BYOC savings. They've been able to save on server management costs, lower energy consumption, increase user productivity, and more—all because they implemented an infrastructure that could adequately support the BYOC model.

Although companies often take on BYOD with an expectation of immediate and prolonged cost savings to the corporation, Mary Brandell (2012) of Network World specifically called out areas where costs after the transition may be higher than expected. In her article, she specifically mentioned that telecom charges are the largest factor that keeps BYOC from being a cost-saving venture in many corporate settings (Brandell, 2012). This concern over telecom charges is applicable to a corporate environment that allows for telecommuting or where employees require data access to their devices while travelling for the company but is not a concern for an educational environment, such as NPS (Brandell, 2012).

Even in environments where the actual hardware purchase cost savings of having employees bring their own laptops, tablets, and phones is negated by increased costs in increasing the network security, infrastructure, and providing wider ranges of support, companies still see benefits of productivity from their workers, if not direct cost savings from their hardware purchases (Twentyman, 2012).

As the business world model of BYOD transitions its way into the academic world, 11 percent of college campuses in the U.S. are transitioning away from providing student computer labs and smart classrooms in a deliberate effort to have students furnish their own laptops for schoolwork (Kolowich, 2010). Christopher Duffy, chief information officer at Pierce College, presented an insight into one reason why educational institutions may be at 11 percent implementation of BYOD (Kolowich, 2010) while the corporate world is at 72 percent (Bring Your Own Device to Work, 2012).

> The problem at Pierce, Duffy says, is not that students don't have their own computers; it's that their machines are often old and sometimes incapable of running the requisite programs. "We're finding these four- or five-year-old laptops that they're trying to run current software," he says, noting that this is probably a common issue on campuses that serve primarily adult learners who cannot necessarily afford to upgrade on a regular basis. (Kolowich, 2010)

Educators try to follow business trends for cost savings, efficiency, and outcomes. According to Intelligent Business Research Services Ltd., "In the last four decades, educational systems have frequently attempted to adopt trends in business to the educational process. The BYOD trend is no exception. Almost all respondents stated that BYOD was a significant trend in education" (Sweeney, 2012).

Most educational institutions that transition to BYOD do not do so for immediate cost savings. Infrastructure requirements often lead to an environment where two systems are being used at once, the traditional school-owned computer paradigm that is currently in place at NPS and another where the students are bringing their own devices to run on the school's network. The second paradigm works off of a secondary network and requires expensive back office server upgrades. The heavy upfront cost of

transitioning to BYOD is recovered over time, if the schools do not want to try to control their students' computers, but the focus of BYOD in education is generally on educational outcomes (Sweeney, 2012).

C. LEGAL CONCERNS

1. Software

There are two major categories of software: system and application. Software licensing plays a big part in setting up a BYOD environment. Software licensing is complicated to understand on its own. The relationship between software licensing and the BYOD environment needs to be thoroughly understood; otherwise, implementation of a BYOD strategy could spell disaster. If one does not understand software, the types, and the rules governing its usage, one could easily find himself or herself doing something unintentional or illegal. Under a BYOD environment, students at the NPS GSBPP would use their personal computing devices to access the client server over a remote access connection to use certain software applications. Virtually, this would give the students the capability to work from anywhere. But a BYOD environment can come with potential problems if not managed properly, including the use of software on a client server. System software is what delivers the basic non–task-specific functions of the computer system, while application software is responsible for controlling the specific command tasks. Therefore, the relationship between the two types of software and their interfaces with the systems hardware is also important to understand (see Figure 1).

Software is instructions and data that direct the computer to accomplish a specified task. Software can be a single program or a collection of programs and data that are packaged together. Determining the right software to use will also help to determine what type of computer you use. System software is accountable for managing and integrating the individual hardware components, such as the central processing unit, random access memory and input/output devices of a particular computer system. This way, other software and the users of the system see it as a functional unit. System software consists of an operating system, file and display managers, management tools, networking, and other fundamental utilities.

Application software such as Skype and video games are used to achieve specific tasks beyond running the computer system, meaning it does not interact with the architecture of the computer but interacts to what the end-user is tasking it with. “This is usually equipped with a single program, like image viewer, a spreadsheet, text or database processing system, or a database management system, which consists of a collection of fundamental programs that may provide some service to different independent applications” (Admin, 2013).

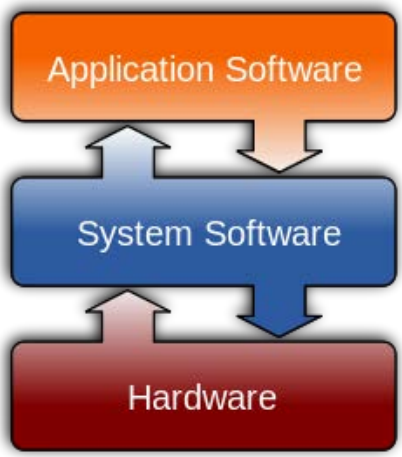

Figure 1. Classification of Software Relationships (from Golftheman, 2012)

In a BYOD environment encountering different licensing requirements for software applications is common a practice. Essentially you are running multi software applications in a server-client or cloud computing environment in which a person has addressed the licensing agreement of each single piece of software.

> In the BYOD context, licensing complexities also multiply. Perhaps most confounding to IT departments are questions related to how the number of connecting users and devices impact what's required from a licensing perspective. The costs and difficulties associated with monitoring this dynamic environment (not to mention the licensing costs themselves) can be significant and must be weighed against the operational efficiencies that can be achieved by migrating to virtualized application delivery models. (Baker, 2012)

Cost can be another factor when it comes to implementing a BYOD policy. Most entities implement a BYOD policy because they feel that it will significantly reduce their

software, hardware, and IT systems cost while still supporting their employees. When operating in an economic downturn or facing budget constraints, the first thing any establishment wants to do is cut costs and save money. However, implementing a BYOD policy solely based on cutting cost might only produce a trade-off in cost. The trade-off might be reducing hardware expenditures to only have increased software expenditures depending on the licensing of the software and network access and architecture delivery method used. Granted, much of the cost is dictated by the environment where a BYOD policy is set up. For a small-business user, the cost savings may be substantial, while larger entities might not see much improvement over their current policy. Software plays a key role in any BYOD program. Therefore, understanding the software licensing and legality will enhance knowledge of software delivery in a BYOD environment.

Computing software has different type of licenses, some of which are copyrighted and licensed under a software license. The end user may be using software that is of a restrictive proprietary nature or open license under the same legal basis of usage. However, not all software is copyrighted or licensed. Therefore, software is generally classified as either proprietary or a free and open source. The hallmark of proprietary software licenses is that the software publisher grants the use of one or more copies of software under the end-user license agreement (EULA), but ownership of those copies remains with the software publisher. This feature of proprietary software licenses means that certain rights regarding the software are reserved by the software publisher. Therefore, it is typical of EULAs to include terms that define the uses of the software, such as the number of installations allowed or the terms of distribution. Free and open-source licenses generally fall into two categories: those with minimal requirements about how the software can be redistributed (permissive licenses), and those that aim to preserve the freedoms given to the users by ensuring that all subsequent users receive those rights (DevTools, 2011–2012).

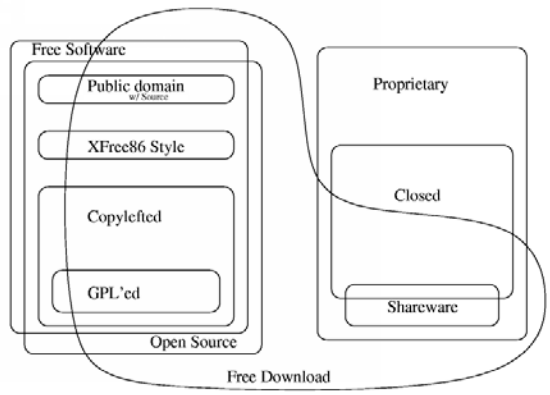

Figure 2. Software Under Various Licenses (from Chao-Kuei, 2010)

As more employee and student-owned computing devices are used in a BYOD environment, the management of software licenses can become more challenging. From a cost perspective, the goal is not to over-purchase licenses but to find a balance to ensure that the program still supports the faculty, staff, and students in an academic environment. There have been software compliance challenges in a BYOD environment. The Federation against Software Theft (FAST) has issued warnings in the past that BYOD can expose entities to risk if employees use illegal software unsupported by the company. For instance, a company may have purchased a valid application license for an employee-owned device, but the employee may still be accessing and using an application without a valid license agreement in place. What can make a situation worse is that the Independent Software Vendors (ISVs) provide no means or reasonable methodology for how software licensing works when their employees use both company and personally owned devices. Some ISVs even offer a per-device license or a per-use license for a given application.

Organizations are taking a number of approaches to address BYOD software licensing issues. These approaches include the following:

- **Establish a corporate enterprise application store.** Tablet and smartphone users are quite familiar with and comfortable using online stores for downloading, installing, and updating consumer apps. Now, organizations are eyeing the same approach for their enterprise apps. In fact, 60 percent of information technology (IT) organizations plan to deploy their own enterprise app stores by 2014 (Gartner, 2011). Such stores would distribute company-approved, secure, malware-free apps to

any type of BYOD device, including desktop computers, laptops, tablets, and smartphones. The benefits of using this approach are that it can help organizations better manage software licenses because the organization can monitor and control the number of licenses in use at any time and ensure that only those users who need certain apps access them, thus reducing the number of licenses needed. (Myers, 2012)

- **Provide access to applications via cloud client computing.** Organizations that have moved to a virtual desktop infrastructure (VDI) can leverage the technology to better manage BYOD licenses. VDI can provide users with secure, dynamic access to corporate applications on a wide range of devices, from personal computers (PCs) to thin clients with no impact to their bandwidth or end-user experience, while allowing the organization to better and more securely manage the end-point devices and software licenses, because the applications are centrally managed on IT servers and delivered virtually through the cloud. (Myers, 2012)
- **Move to a cloud model.** Cloud delivery models for software applications have gained in popularity over the last 10 years. Many organizations already use Software as a Service (SaaS) for e-mail, as well as cloud-based applications like Salesforce.com. And many are eyeing Google Apps for Business and the recently released Microsoft Office 365 Preview to provide office productivity, calendaring, and collaboration solutions to their users. The benefit of an SaaS or cloud-based offering is that a user can access business-critical apps from either a personal device or an office computer, while the company pays for one seat. (Myers, 2012)

2. Cloud Computing and Thin-client Server

Definitions for cloud computing vary based on an entity's own scientific or technical definition. One simple and undiluted definition is that cloud computing is another way for an entity, corporate or educational, to deliver a program application to end users over a network, giving them the ability to run a program on several connected computing devices at the same time. It is up to the organization to understand its needs and determine whether using the cloud as a streamline best fits the organizational policy. For instance, in an educational setting, cloud computing might be best used for distance learning. Distance learning has been growing over the past few years, helping those who are older or may not be able to travel to colleges because of family or job concerns. With the Internet readily available to many households, this gives them a non-traditional way of earning a degree in higher education.

For instance, the University of Florida uses distance learning to broadcast lectures where no lecture hall could possibly hold them. They also offer dozens of popular courses such as biology, psychology, and statistics online. Online education is best known for serving older, non-traditional students who cannot travel to colleges because of schedules with jobs and family. In a world of declining funding, budget cuts, and other constraints, technology has enabled campuses, such as some brick-and-mortar campuses, to still provide distance learning courses (Gabrial, 2010).

At the University of Florida, resident students are earning 12 percent of their credit hours online this semester, a figure expected to grow to 25 percent in five years. According to the Sloan Survey of Online Learning, online education is exploding: 4.6 million students took a college-level online course during fall 2008, up 17 percent from a year earlier. Colleges and universities, mostly public, that have plunged into the online field cite their dual missions to serve as many students as possible while remaining affordable and still exploiting the latest technologies. At the University of Iowa, as many as 10 percent of 14,000 liberal arts undergraduates take an online course each semester, including Classical Mythology and Introduction to American Politics. At the University of North Carolina at Chapel Hill, first-year Spanish students are no longer offered a face-to-face class; the university has moved all instruction online, despite internal research showing that online students do slightly less well in grammar and speaking (Gabrial, 2010).

The fact is that distance learning has grown exponentially. However, to meet the demands to support faculty and students to maintain academic standards, distance learning programs require constant innovation and optimization both to infrastructure and delivery of software to the end user. Cloud computing offers a balance and a way to provide such resources in education. Understanding cloud computing also requires understanding the type of services offered by cloud computing.

Understanding a streamlined structure of users in an IT-provided–services environment in a typical university is important when trying to understand how IT provides services (see Figure 3). The IT services department takes care of all the demand for IT services by providing students, faculty, and staff with software (e.g., e-mail

accounts, productivity applications, and anti-virus) and hardware (e.g., PCs). They also provide researchers and students with any special software and hardware for running in experimental labs. Last, the IT services department provides web developers with the necessary development tools and applications needed for web hosting services (Sultan, 2010).

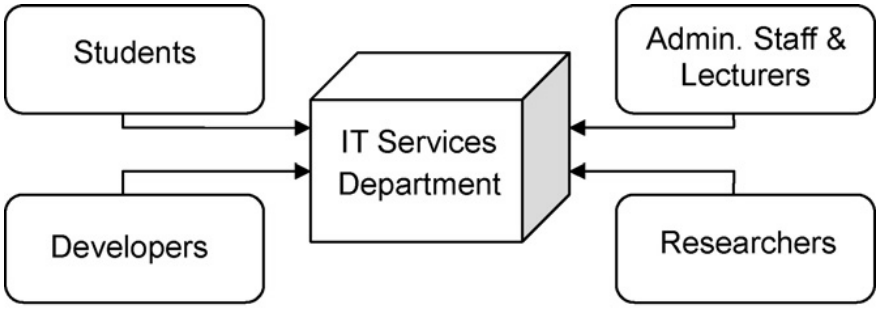

Figure 3. Simplified Structure of Main Users of IT Services (from Sultan, 2010)

However, there is also a basic structure of users in a typical university that may use the services of cloud computing (see Figure 4). Students, faulty, and staff use the services accessed through thin clients of providers of SaaS and Infrastructure-as-a-Service (IaaS) clouds. Software used in this setting by any of the end users resides on the servers of the SaaS cloud provider online. The IaaS cloud provider would also provide disk space and any additional hardware needed online.

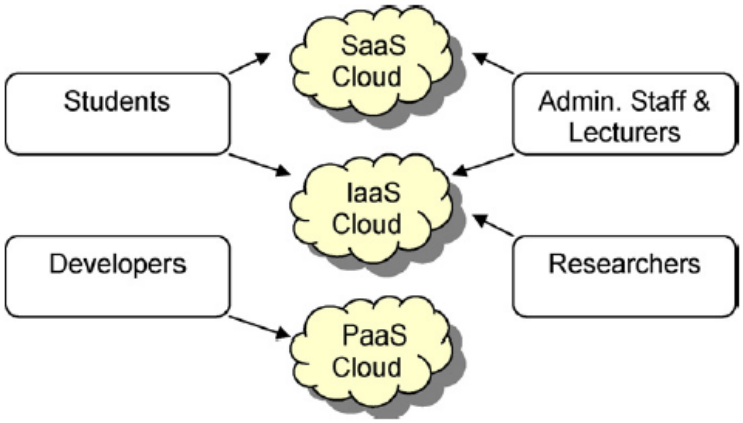

Figure 4. Simplified Structure of Main Users of IT Services (from Sultan, 2010)

Conversely, by understanding the types of services offered by cloud computing, one begins to understand what provided IT services under each environment means for campus infrastructure. The following list identifies the three main types of services that can be offered by the cloud.

- **Infrastructure as a Service (IaaS):** Products offered via this model include the remote delivery (through the Internet) of a full computer infrastructure (e.g., virtual computers, servers, and storage devices).
- **Platform as a Service (PaaS):** Remembering the traditional computing model where each application managed locally required hardware, an operating system, a database, middleware, Web servers, and other software will help in understanding this cloud computing layer. Also a team of network, database, and system management experts is needed to keep everything up and running. With cloud computing, these services are now provided remotely by cloud providers under this layer.
- **Software as a Service (SaaS):** Under this layer, applications are delivered through the medium of the Internet as a service. Instead of installing and maintaining software, users simply access it via the Internet, freeing themselves from complex software and hardware management. This type of cloud service offers a complete application functionality that ranges from productivity (e.g., Microsoft Office) applications to programs such as those for Customer Relationship Management or enterprise-resource management (Sultan, 2010).

Before cloud computing made its way to the scene, the client–server computing model was used and continues to be used to deliver applications not installed on the end user's (client's) computing device. It was also designed to provide flexibility, help IT management, and move away from mainframe computing. Just like cloud, it is all based on the concept of directly running the software application not on a personal computer, but on a dedicated file server. The computing device simply acts as a virtual window using a user interface to run the application.

The client–server model (see Figure 5) was used because one does not have to install the application on a device, which makes it a cheaper and more convenient option. It also allowed users to run the program virtually from anywhere. Like cloud computing, client–server computing also has been defined in many ways.

> The big difference between cloud and client–server development is in what you know: in traditional client–server systems, you might have a specific computer that is your server, and that's where your stuff is running. The computer may not

be sitting on your desk in front of you, but you know where it is. In the cloud, you aren't confined to a specific server. You have computing resources—that is; someone is renting you a certain amount of computation on some collection of computers somewhere. You don't know where they are; you don't know what kind of computers they are. You could have two massive machines with 32 processors each and 64 gigabytes of memory; or they could be 64 dinky little single-processor machines with 2 gigabytes of memory. The computers where you run your program could have great big disks of their own, or they could be diskless machines accessing storage on dedicated storage servers. To you, as a user of the cloud, that doesn't matter. You've got the resources you pay for, and where they are makes no difference as long as you get what you need. (Computing Tech, 2011)

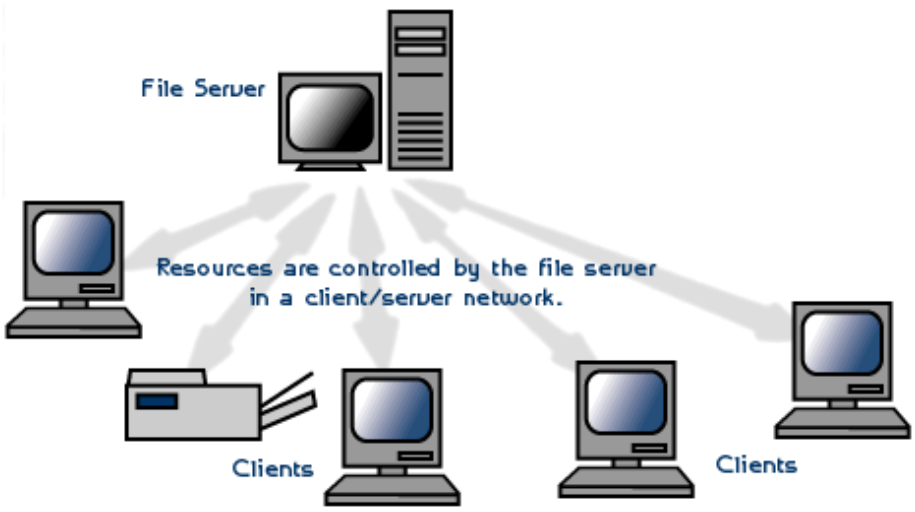

Figure 5. Client–Server Network (from Winkelman, 2013)

Just like in a cloud computing environment, there are also rules to abide by when it comes to a client–server model. The fact is that there are many applications with source codes constructed to run and operate in a client–server set-up. Many applications that are Internet based such as e-mail, web browsers, and e-readers are good examples. Then there are applications that were constructed not to run in a client–server set-up, such as certain Microsoft products. Whatever the computing structure, running software applications still plays an important role. Early on, license types were discussed minimally to demonstrate the complexity of how software licenses are made up. Understanding the licensing schemes will help in choosing the right application or system software to use in a BYOD environment, and this is regardless of what computing

method used. Licensing schemes for software depend on two things: its intended market, and architecture. Understanding these schemes will also help understanding legally what can and cannot be done perhaps with existing software applications currently being used or that will be used in a new or existing BYOD environment.

3. Types of Licenses

a. Per-User License

A per-user license is tied to a particular person and is most popular with web and desktop applications. With a per-user license desktop application, in certain occasions there exist the ability to install this type of software on multiple computers at once, with the caveat that the software is only be used by one person (GurockSoftware, 2011). A good example of a license per user system application is Windows Server 2003.

b. Per-Computer License

A per-computer license allows the end user to install and use the given software on one computer. If the intent is to use it on more than one computer, then multiple licenses are needed. However, multiple users can use the software if they are doing so on the same computer (GurockSoftware, 2011). A good example of a license per computer desktop software application is Microsoft Office 2013 productivity suite.

c. Per-Client License

A per-client license usually is used in client–server architectures. In most cases, there is a need to acquire a license for each client called the client access license (CAL). And in most cases, an enterprise also needs additional server licenses because Microsoft requires that all clients who connect to the server have a license both to connect to the server and to use the software application (GurockSoftware, 2011).

d. No-Fees-at-All License

No-fees-at-all licenses are commonly used with open-source or freeware software. Free software applications can be very useful for marketing (GurockSoftware, 2011).

e. Floating License

A floating license provides the capability to use software on multiple computers by multiple users. The caveat is that only one user is using that license at any one given time. In most cases, floating licenses are bundled with other software, so when purchasing expensive software that is necessary but potentially underutilized, a floating license can help defer extra cost (GurockSoftware, 2011).

Although this is not an all-inclusive list of licensing schemes, it does give a picture of how complicated understanding software and system applications can be. What is even more complex is understanding the full nature of what CALs and management licenses (MLs) are under volume licenses programs. First, we discuss CALs and MLs as prevalent to Microsoft, which can be complicated based on the technical nature of licensing alone.

> Under the realm of Client-Access Licenses you have user CALs and Device CALs (Microsoft, 2013; see Figures 6 and 7). While CALs might be priced the same they have different access rights therefore identifying usage needs upfront can help save cost by choosing the best option. With the User CAL, you purchase a CAL for every user who accesses the server to use services such as file storage or printing, regardless of the number of devices they use for that access. Purchasing a User CAL might make more sense if your company employees need to have roaming access to the corporate network using multiple devices, or from unknown devices, or simply have more devices than users in your organization. (Microsoft, 2013)

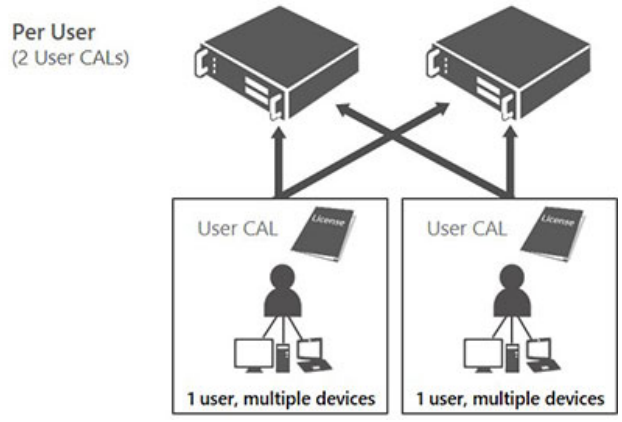

Figure 6. Client Access License User (from Microsoft, 2013)

User CALs can be costly if you have to purchase one for each student, since it only allows one user to connect to the server. This means that any student can connect, but only one student may use a given CAL at any given time. So determining if this is best suited in a GSBPP BYOD environment will be critical in the planning phase.

> Device CALs operate much in the same way as user CALs with limitations place on connections made by devices vice users. A single CAL will enable once device to connect and user software on the client-server regardless of connected users. With a Device CAL, you purchase a CAL for every device that accesses your server, regardless of the number of users who use that device to access the server. Device CALs may make more economic and administrative sense if your company has workers who share devices, for example, on different work shifts" (Microsoft, 2013).

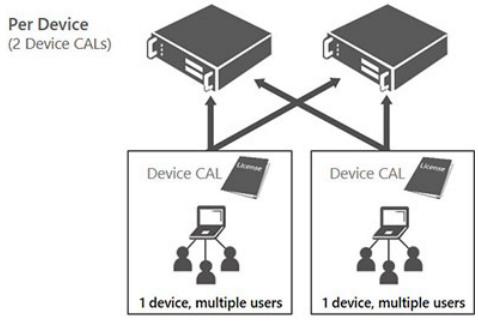

Figure 7. Client Access License Device (from Microsoft, 2013)

CALs allow client computers to legally connect to server software. The choice to choose between ether a user or device is left to the individual consumer to decide based on the best case scenario, requirements, and needs. Although being both priced similarly the same CALs are not interchangeable therefore switching requires the purchases of new or additional CALs, which can be a costly depending on the amount of end-users that require access.

Then there are operating system environments (OSEs) and machine licenses (MLs). An operating system environment is the instance of an operating system that can be virtual. There are two types of MLs, client and server that are required for devices that run server OSEs. However, with server MLs license are based on the number of physical processors.

> Under the Management Servers licensing model [see Figure 8], you must acquire and assign the required number of appropriate category (server and/or client) and type (OSE and/or User) of ML to the device on which OSEs are to be managed. Included with the ML are the rights to run the corresponding management server software, so you do not need to acquire separate licenses for the management server software (Microsoft, 2013).

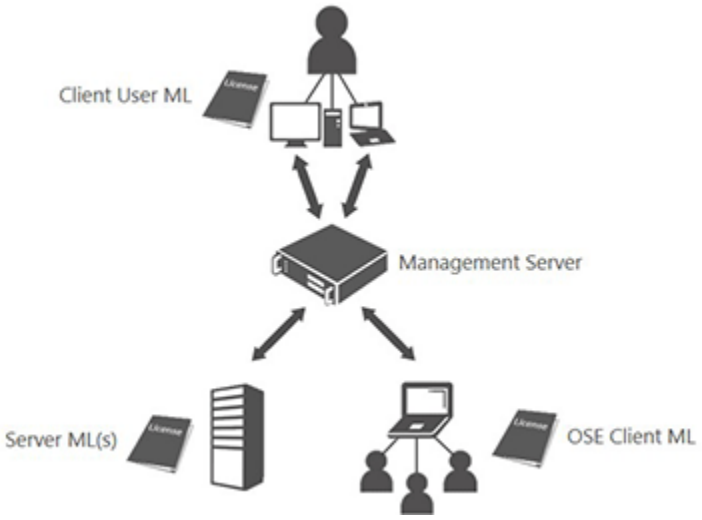

Figure 8. Management Server Licensing (from Microsoft, 2013)

While CALs licenses might be much more pertinent to one running a thin-client server, MLs would be conducive if the decision was made to run a enterprise management automation software tool such as Microsoft Data Center 2012. And while it offers client management helping with compliance and control it might be more conducive to much larger enterprises or if utilizing cloud-computing.

Management of every single software application license agreement that is running on a server needs to be tracked. Software license management is either a process or software tool that can be used to control and document how or where the software application is running. These management tools help to enforce and ensure compliancy with each software EULA.

Software management also plays a key role in ensuring that software licenses are in compliance, even in server–client and cloud environments. There is currently a lack of standards-based practices and supporting tools to consistently describe licensed products and product usage. The emergence of cloud computing along with

virtualization adds additional complexity to software license management for customers, platform vendors, and application providers (Distributed Management Task Force [DMTF], 2011).

Software and system application licenses used in a virtual environment must be managed with the same criteria and just as thoroughly as if they were on a physical server. Understanding the EULA from the software manufacturer also helps determine what actions to take with software in a server environment. Users should read their software manufacturers' license agreements carefully to determine whether virtual licenses are specifically addressed in the contract. "If software is licensed "per seat," and virtual licenses are NOT specifically addressed in the EULA, you should verify with the manufacturer that each virtual machine requires its own license, as well as any machine that accesses it" (Kelsey, 2012).

A more in-depth synopsis about the EULA is that it acts as an agreement between the software provider and end user, restricting what the end user can and cannot do with the given software. In some instances, it can restrict the redistribution of the software or prohibit reverse-engineering of it, while also giving certain usage rights to the user. The EULA was once a traditional paper contract, but much of the software used today is distributed via the Internet, meaning that physical contracts have become far and few between, unless, of course, all purchased software in contracted out. This means that on most software today, there is a EULA screen prior to installing the program.

There are still debates about the enforceability of such contracts for the individual home user; however, an electronic EULA does provide legal protection to software distributors. It is seen in a windows pop-up before you install any new piece of software application, but is it fully read? In some cases scrolling 70 pages gets you to the magic words of "I agree" or "agree." However, the consumer has to understand what the agreement was, and if anything at all, its legality.

> The original purpose of a EULA was to protect software developers and distributors from having their products unlawfully distributed, that goal is now only a small part of most EULA's. A EULA might also contain a clause that allows the software to monitor your computer usage,

> automatically update itself when connected to the Internet, or disable certain features as deemed appropriate by the software vendor. (Cohen, 2011)

In not reading the EULA prior to its installation, the end user could very well agree to the monitoring of their activities and informing its programmers about them.

> However, probably one of the most common EULA terms today regards distributor's damage liability. The United States, the European Union, and most other government bodies have laws that protect consumers from damage done to them by equipment or software they purchase. The EULA of most common software today removes this protection. Thus, improperly coded software, or even malicious software, can damage your computer and the distributors are released from all liability. (Cohen, 2011)

4. Software Applications

We looked at the license and service agreements from three software vendors pertinent to our needs. We looked at StataCorp's Stata/IC Data Analysis and Statistical Software, Frontline's Solvers-Risk Solver Platform, and Oracle's Crystal Ball. Stata I/C is a statistical software that provides tools for data analysis, data management, and graphics and comes in a complete package as opposed to individual modules. It is available with either a perpetual license (no expiration) or an annual license. However, the company does offer educational licenses options, such as single user (identified-user license), network (concurrent use), volume (bundle of single users at the same time), compute-server (installed and run on one machine), term (expires after one year), and student lab (for a minimum of 10 concurrent users, installed on either a network or 10 individual computers).

Under the StataCorp software EULA, licenses were broken down by single-user and concurrent authorized-user grant.

a. Single-User License Grant

Single-user license grant applies only to an individual customer whose license and activation key issued by StataCorp specifies the license type as "single user." A single-user license is for a named individual who is identified as the only authorized

user. Under this agreement, StataCorp grants the customer a non-assignable, nontransferable license, without the right to sublicense, and solely for the customer's internal business, research, or educational purposes, and solely by the individual customer. The individual customer is allowed to install up to three copies of the licensed software, only if that individual customer is the sole user of each copy (Stata, 2013).

b. Concurrent Authorized-User Grant

(1) Network License Grant—Licensed Software. According to Stata (2013):

> This Section 2.2(b) (i) applies only to a Customer whose License and Activation Key issued by StataCorp specifies the 'License Type' as 'Network.' Subject to the terms and conditions of this Agreement, StataCorp grants to Customer a non-assignable, nontransferable license, without the right to sublicense, to use the Licensed Software, in object-code form only, within a single local geographic location or physical site solely for Customer's internal business, research, or educational purposes. Customer is authorized by StataCorp to install the Licensed Software on an unlimited number of machines as long as the specific number of Concurrent Authorized Users for which Customer has paid the applicable License Fee is not exceeded. (Stata, 2013)

(2) Compute-Server License Grant—Licensed Software. According to Stata (2013):

> This Section 2.2(b) (ii) applies only to a Customer whose License and Activation Key issued by StataCorp specifies the 'License Type' as 'Compute Server' [*sic*]. Subject to the terms and conditions of this Agreement, StataCorp grants to Customer a non-assignable, nontransferable license, without the right to sublicense, to use and execute the Licensed Software, in object-code form only, installed on a single compute server solely for Customer's internal business, research, or educational purposes. Customer is authorized by StataCorp to install the Licensed Software on only one compute server or one node of a cluster solely for the use of the specific number of Concurrent Authorized Users for which Customer has paid the applicable License Fee. (Stata, 2013)

(3) Student Lab License Grant—Licensed Software. According to Stata (2013):

> This Section 2.2(b) (iii) applies only to a Customer whose License and Activation Key issued by StataCorp specifies the 'License Type' as 'Student Lab'. Subject to the terms and conditions of this Agreement, StataCorp grants to Customer a non-assignable, nontransferable license, without the right to sublicense, to use the Licensed Software, in object-code form only, solely in an educational student lab environment for teaching purposes (but not for research purposes) within a degree-granting institution. Customer is authorized to install the Licensed Software on an unlimited number of machines as long as the specific number of Concurrent Authorized Users for which Customer has paid the applicable License Fee is not exceeded. (Stata, 2013).

Regardless of how tedious it is to read through any EULA or service license agreement, the end user (customer) of the product should look for any restrictions placed on them. As listed in the EULA for StataCorp, the restrictions placed on customers include not being permitted to reverse compile, engineer, or derive the source code of the software. Modifying, renting, commercializing, and any other transfer rights without explicit permission under the agreement were also prohibited. However, this is common verbiage in EULAs. Overall, from reading the EULA, the derived conclusion is if the intent is to operate in a server–client or networked environment, then a "network" Stata I/C license or "student lab" license would be the legal way of doing so. However, it took numerous readings to come to that conclusion, which is why it is crucial in understanding a software package's EULA (Stata, 2013).

Frontline's Risk Solver Platform was the second application that we looked at. It is a risk analysis, simulation, and optimization Excel software tool. Risk Solver Platform offers Monte Carlo simulation, decision trees, powerful conventional optimization, simulation optimization, and stochastic optimization capabilities for problems of virtually any size (Frontline Solvers, 2013). The license agreement was not as long-structured as with StataCorp's and Oracle's, but it addressed the service license and restrictions as expected. Frontline's systems software agreement addressed the following licenses.

> **5. Evaluation License**
>
> If and when offered by Frontline, on a one-time basis only, for a Limited Term determined by Frontline in its sole discretion, Licensee [*sic*] may

Use [*sic*] the Software on one computer (the 'PC'), and Frontline will provide Licensee with a license code enabling such Use [*sic*]. The Software must be stored only on the PC. An Evaluation License may not be transferred to a different PC. (Frontline Solvers, 2013)

6. Standalone License

Upon Frontline's receipt of payment from Licensee [*sic*] of the applicable Fee for a single-Use [*sic*] license ('Standalone License'), Licensee may Use the Software for a Permanent Term on one computer (the 'PC'), and Frontline will provide Licensee with a license code enabling such Use. The Software may be stored on one or more computers, servers or storage devices, but it may be Used [*sic*] only on the PC. If the PC fails in a manner such that Use [*sic*] is no longer possible, Frontline will provide Licensee with a new license code, enabling Use [*sic*] on a repaired or replaced PC, at no charge. A Standalone License may be transferred to a different PC while the first PC remains in operation only if (i) Licensee requests a new license code from Frontline, (ii) Licensee certifies in writing that the Software will no longer be Used [*sic*] on the first PC, and (iii) Licensee pays a license transfer fee, unless such fee is waived in writing by Frontline in its sole discretion Licensee may use the software for a permanent term on one computer, and Frontline will provide Licensee with a license code enabling such Use. (Frontline Solvers, 2013)

7. Flexible Use License

Upon Frontline's receipt of payment from Licensee of the applicable Fee for a multi-Use [*sic*] license ('Flexible Use License'), Licensee may Use the Software for a Permanent Term on a group of several computers as provided in this section, and Frontline will provide Licensee with a license code enabling such Use [*sic*]. The Software may be stored on one or more computers, servers or storage devices interconnected by any networking technology that supports the TCP/IP protocol (a 'Network'), copied into the memory of, and Used [*sic*] on, any of the computers on the Network, provided that only one Use occurs at any given time, for each Flexible Use License purchased by Licensee. Frontline will provide to Licensee (under separate license) and Licensee must install and run License Server software ('LSS') on one of the computers on the Network (the 'LS'); other computers will temporarily obtain the right to Use the Software from the LS. If the LS fails in a manner such that the LSS cannot be run, Frontline will provide Licensee with a new license code, enabling Use on a repaired or replaced LS, at no charge. A Flexible Use License may be transferred to a different LS while the first LS remains in operation only if (i) Licensee requests a new license code from Frontline, (ii) Licensee certifies in writing that the LSS will no longer be run on the first LS, and (iii)

> Licensee pays a license transfer fee, unless such fee is waived by Frontline in its sole discretion. (Frontline Solvers, 2013)
>
> Much like the EULA restrictions seen in StataCorp, the same restrictions appear in the service agreement for Frontline's system software, with the notable exception that merging the software into any other software or using the software to develop any application or program having the same primary function as the Software is prohibited (Frontline Solver, 2013).

Another simulation, optimization, and risk analysis Excel software tool that is readily used is Oracle's Crystal Ball. Oracle Crystal Ball is the leading spreadsheet-based application for predictive modeling, forecasting, simulation, and optimization. It gives unparalleled insight into the critical factors affecting risk, helping users to make the right tactical decisions to reach their objectives and gain a competitive edge in uncertain market conditions (Oracle, 2013). The focus on Oracle Crystal Ball licenses was based on the academic versions offered.

If the program or license type is identified as one of the following, other rights and limitations apply as follows:

> **8. Academic License**
>
> If the program and license is identified as Academic Edition ('AE program'), only a qualified education licensee may use the AE program. Qualified Education Licensee shall mean (i) an accredited higher education institution; (ii) a teacher or professor of an accredited higher education institution; or (iii) a current full- or part-time student of an accredited higher education institution with proof of enrollment. Proof of enrollment must either be a copy of an official photo identification care from the accredited higher education institution or official documentation from the accredited higher education institution's registration office verifying that the individual is an enrolled student at the institution at the time of the license. If the official identification card does not include a photograph of the student, the copy of the identification card must be accompanies by a second source photo identification. Any user that is not a qualified educational licensee and is using the AE program has no rights under the [Crystal Ball License Service Agreement] CBLSA. AE programs may only be used in conjunction with the classes or work related to the accredited higher education institution and shall not be used for any commercial purposes. Oracle shall resolve any issues relating to the eligibility or determination of a qualified education licensee in its sole discretion. The AE program may be time-sensitive and if so, will expire

in the number of days set forth in the invoice from Oracle. After expiration, further installations will be prevented without an appropriate license file issued from Oracle. (Oracle, 2013)

9. Academic Lab License

Only Qualified Education Licenses may obtain an Academic Lab license. Any user that is not a qualified educational licensee as defined in 1 above and is using an Academic Lab license has no rights under this CBLSA. If a Qualified Education Licensee has obtained an Academic Lab license, such Qualified Education Licensee may install and use the program on as many computers as the Qualified Education Licensee has purchased licenses for as indicated on the ordering document from Oracle. The Academic Lab license is not a perpetual license, but is time-sensitive and may either expire in (i) 1- year from installation, or (ii) a number of days as determined by Oracle upon issuance of the license file. (Oracle, 2013)

10. Textbook License

If the program is identified as Textbook Edition or the program license is pursuant to the purchase of a textbook ('TB license'). The textbook license is not a perpetual license, but is time-sensitive and may either expire in (i) 140 days from the date of installation, or (ii) as otherwise set forth in the documentation accompanying the TB license. After expiration further installations are prevented without an appropriate license file issues from Oracle. Textbook Edition programs may not be used for any commercial purposes. (Oracle, 2013)

11. Trial or Evaluation License

If the program was activated pursuant to a trial or evaluation license, the trial or evaluation program is not a perpetual license, but is time-sensitive, and may either expire in (i) 30 days from installation, or (ii) a number of days as determined by Oracle upon issuance of the license file. After expiration, further installations are prevented without an appropriate license file issued from Oracle. Only one trial or evaluation license will be issued per user, unless otherwise provided by Oracle. Oracle may revoke the use of trial or evaluation programs at any time and for any reason. (Oracle, 2013)

12. Remote Access Technologies

You may use remote access technologies, such as Microsoft ® [*sic*] Windows ® [*sic*] Terminal Server or Citrix ® [*sic*] Metaframe ® [*sic*], for an authorized user to make use of the programs, provided that only the authorized user of the computer hosting the remote access session accesses and uses the program with a remote access computer. These remote

> access rights do not permit you to use the program on both the computer hosting the remote access sessions and the computer accessing the program at the same time. No technical support shall be provided with respect to such remote access technologies. (Oracle, 2013)

As seen with the other user agreements, the same standard language of prohibiting reverse engineering or decompiling of the software was also present. Beyond that, EULA was not as definable as the other two service agreements that we researched.

But knowing what is in the EULA of every application or how system software is intended to be used is important. In the event that a licensee violates one or more terms of a EULA, a software company may wish to sue the end user or licensee for breach of contract. Licensors generally have little trouble establishing the enforceability of a EULA negotiated between it and the licensee. However, court rulings on the enforceability of certain types of boilerplate EULAs against licensees vary among jurisdictions. For instance, courts in California are likely to find most EULAs enforceable.

In the age of the shrink-wrap EULAs, there is enforceability:

> The enforceability of an EULA may depend on whether it was negotiated directly between the licensor and the user, or whether the license was a "shrink-wrap" or "click-wrap" license, which users accept by opening the software packaging, or by downloading or installing the software. Some courts have found these to be unenforceable contracts of adhesion, while others have ruled them to be valid and enforceable. The trend appears to be in favor of enforcement. The Ninth Circuit, which includes California, has ruled in favor of enforceability. (Kabak, 2013)

In the case of all three software applications we researched, the EULA was clear in its ability to define the fundamentals of the environment in which the software application can operate. However, it might not always be that clear and concise, or instances where there is lack of data needed to make the best determination. The biggest criticism of EULAs is that they are lengthy enough to where the end users will not thoroughly read through them. A good example is iTunes, which once had a EULA that was 56 pages long. If an enterprise or school is going to be operating in an environment that requires comprehensive software licenses management, or if there is ever doubt as to

whether a license is valid enough to operate in a client–server architecture, cloud computing, or on multiple computers, it is simply best to call the company for any legal clarification.

D. LESSONS LEARNED

The implementation of BYOD is making significant changes on the campuses of countless colleges and universities around the country and even the world. Many students have been using their own technology at these educational institutions since the early 2000s, and schools simply cannot block the trend. By permitting students to bring personally owned mobile devices, laptops, tablets, and smartphones to their learning environments and use those devices to access privileged information and applications, school administrations believe that BYOD may help their students be more productive (Daly, 2013a). Additionally, allowing students to use their own devices increases student morale and convenience, while making the school appear more a flexible and more positive educational setting.

In 2012, a BYOD survey was conducted with more than 500 IT professionals from colleges and universities across the United States and the United Kingdom. The survey fielded questions relating to how BYOD was being used, security challenges, and potential growth moving forward (Daly, 2013a). The results revealed significant statistics regarding BYOD's landscape among schools, indicating that there is great opportunity for students and professors, as well as enormous risk. Figure 9 presents the major takeaways of the educational institutions surveyed.

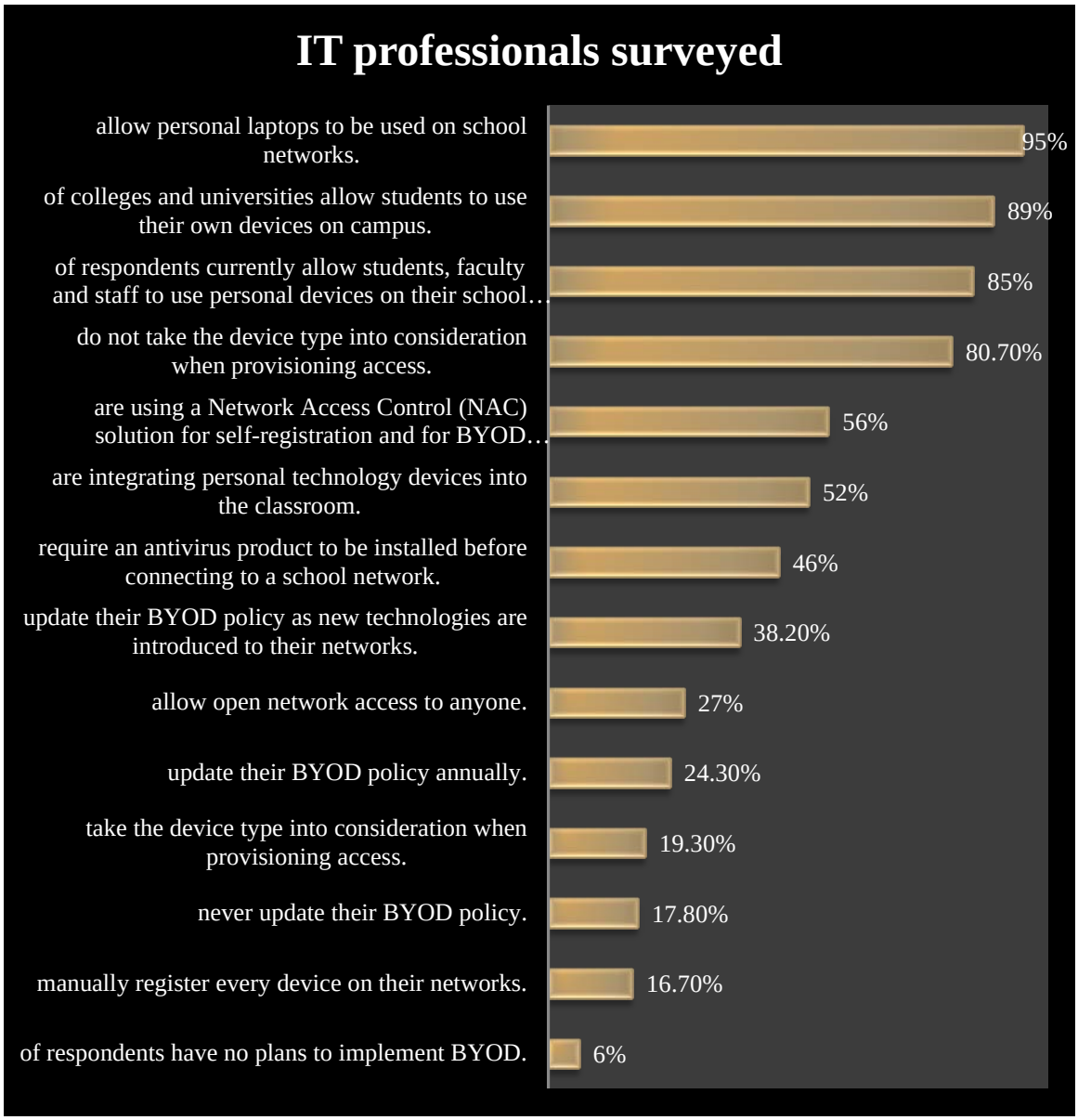

Figure 9. Significant Bring-Your-Own-Device Statistics of 500 Colleges and Universities (from Daly, 2013a)

One of the most notable facts in Figure 9 is that 85 percent of educational institutions allow students, teachers, and faculty to use personal devices on school networks. This statistic represents a huge opportunity for professors and students to engage in new learning styles (Daly, 2013a). This survey is one example of the ample guidance that is being offered for those interested in BYOD. Through the perspective gained as a result of trial and error, many lessons learned can be noteworthy for college

IT and administrative staff departments prior to converting to a full-on BYOD setting. We discovered in our research that the following topics were among the most influential for other colleges and universities who have already made the BYOD transition:

- student IT agenda,
- supporting network,
- faculty support, and
- security concerns.

These lessons learned can help interested parties adapt more quickly to the technological changes that derive from BYOD implementation.

1. Student Information Technology Agenda

In today's academic culture, students are much more demanding when it comes the technology they wish to use to complete their academic requirements. Perhaps five to 10 years ago, students would seek advice from academic departments on which computing products would benefit them the most in class. However, today's generation of college students is much more technologically savvy and demand that their own mobile computing device, whichever one that may be, satisfies both their personal and academic needs. According to one article, "Indeed, Student Monitor, a provider of college student–centric market research services, found that 88 percent of students access the web every day to do research, engage in social networking, check e-mail, text friends, collaborate or create content" (CDW-G, 2012).

With the widespread availability of computer technology increasing daily, mobile devices are beginning to become students' primary means of computing on most college and university campuses. At the University of Tennessee in Knoxville, "27,500 students and 9,700 faculty and staff members have registered 75,000 devices for use on the university's wireless network, which averages out to 2.1 devices per user. (Some institutions have reported device-to student ratios as high as 3.5-to-1)" (CDW-G, 2012). At the University of Kentucky, chief technology officer Doyle Friskney believes that "this student-driven model has become so infused in the campus culture that it's become impossible to institutionally direct and control. Indeed, in many ways, students are now

setting the IT agenda" (CDW-G, 2012). Even though many questions regarding technological changes across campuses nationwide are still in the process of being answered, it is evident that schools that fail to keep pace with students' craving for the latest in computing capability will begin to appear unattractive.

Often, students relate a school's technology as a key item to their academic success and expect their schools to support this need. According to the *21st Century Campus Report*, "87 percent of current college students considered technology offerings when deciding which institution to attend. And 92 percent of current high school students said that technology will be a key differentiator during their university selection process" (CDW-G, 2012). A BYOD environment offers much more than just the convenience of using one's own device. Institutions that have proven successful in their transition to BYOD have included several advantages aimed directly at students. According to CDW-G (2012), BYOD:

> *Enables technology-rich classrooms:* Technology is slowly being adopted into college and university curricula. Notably, 31 percentof students used technology as a learning tool while in class in 2011 (up from 19 percent in 2010). Pervasive BYOD will help foster this trend, as faculty will be able to assume that most students have access to mobile computing devices and have confidence that the requisite wireless bandwidth is available to support them.
>
> *Initiates new ways of learning:* According to Lee Rainie, director of the Pew Research Center's Internet & American Life Project, mobility and wireless connectivity are creating new kinds of learners who are more self-directed in their acquisition and sharing of knowledge, more inclined to collaborate, and more reliant on feedback.
>
> *Increases student engagement:* Students who use their own personal devices for anytime/anywhere access will engage more in classroom activities, collaborate more fully with classmates, communicate with faculty and learn how to solve problems using the latest skills. (CDW-G, 2012)

Mobile applications are another support milestone that colleges and universities must consider when developing their student computing support structure. Students who have access to multiple computing devices tend to utilize all of them, given whichever is more convenient with regards to their current task at hand. For example, students at NPS

may utilize the computers located in Dudley Knox Library to print out an assignment on their way to class but use their cell phones the next morning to check in via the NPS muster page. In order for schools to accommodate their students with 24-7 access from any mobile device, schools must "mobile-enable" their institutional resources to work with various types of operating systems and hardware platforms (CDW-G, 2012). In addition, "Campuses are moving forward, but progress is slow, says Dr. Susan Grajek, vice president for data, research and analytics at the EDUCAUSE Center for Applied Research [ECAR]" (CDW-G, 2012). According to a recent ECAR's information technology report:

> ECAR's Mobile IT in Higher Education, 2011 report found that a few institutions have mobile-enabled some campus services, particularly those that meet student or public needs, but 38 percent have made no progress in this area. Campuses that have created mobile applications are focusing their efforts in specific areas. (CDW-G, 2012)

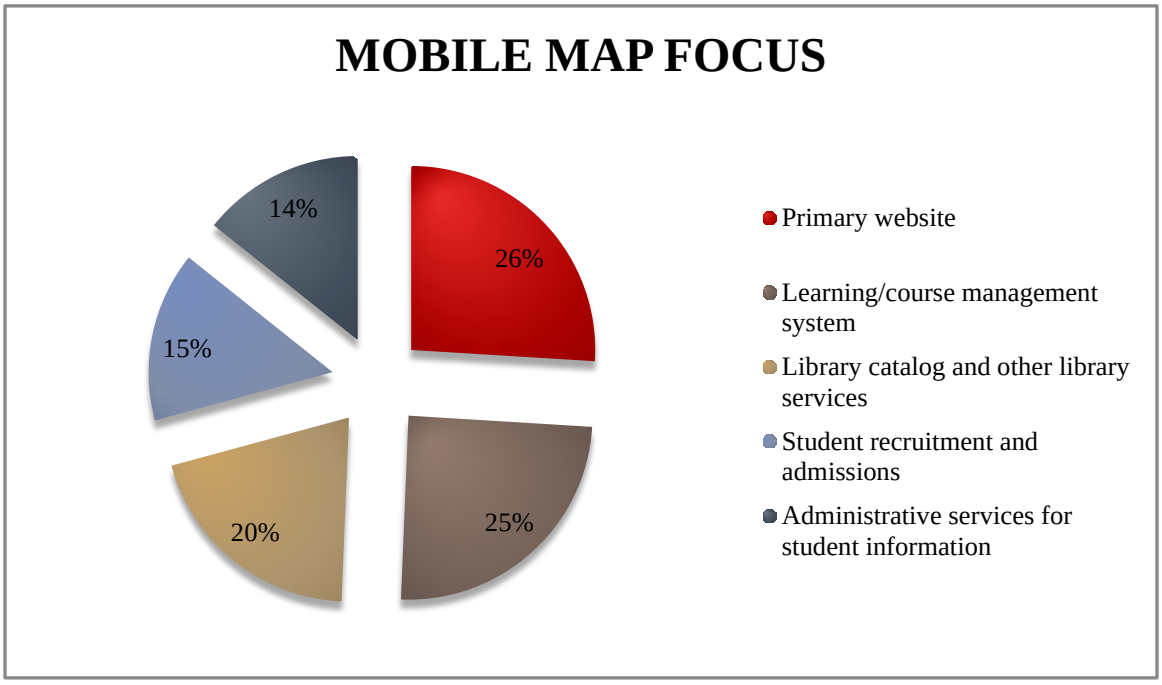

Figure 10. Mobile Map Focus for Mobile-Enabled Campuses (from CDW-G, 2012)

Not all, however, support advances in computing technology. Many colleges and universities have existing computer labs, which are very much utilized consistently by

their students who would not like to see them go away. Currently, there are several factors that benefit students in engaging computer labs versus owning their own devices. Among the many expenses college students must incur, the cost of a new mobile device may not be within their budget. Many schools have a fair number of students who still utilize older technology but struggle to get by due to the limited processing power necessary to run updated applications (CDW-G, 2012). High-end computing for students in technical fields of study is a great example of this. Specialized applications for a variety of engineering, mathematics, or architecture courses may not be affordable to users. Thus, they are relying on the academic departments to provide this capability within computer labs (CDW-G, 2012). Lastly, the convenience of computer labs has always been popular. The idea of collaborating with students who share common interests in their studies is a great way to meet new people and network. Additionally, with everyone in the labs having equal computing capability, it makes working together that much simpler.

2. Supporting Network

Since the beginning of the twenty-first century, colleges and universities have been adapting their networks and policies to accommodate the BYOD movement. Graduate students have been bringing their own wireless-enabled notebooks and personal mobile computing devices with the expectation of their school providing unlimited and reliable wireless connectivity. With an overwhelming number of devices and demand to use these devices to access the network and its resources in real time, many colleges and universities are struggling to meet these expectations (CDW-G, 2012).

The biggest BYOD-related network challenge that many campus IT leaders face is providing sufficient bandwidth. According to Kenneth C. Green, founding director of the Campus Computing Project:

> …as mobile learning devices are integrated into the curricula and campus life, users who have come to think that 24x7 [*sic*] wireless connectivity is a right and not a privilege will have zero tolerance for a network that slows markedly during peak usage or becomes unavailable to them. (CDW-G, 2012)

Additionally, most institutions need to take into account the increasing use of bandwidth to satisfy bandwidth intensive activities. Social networking, video streaming, and multimedia actions are vastly growing in today's culture and are often essential to meet academic and personal needs (CDW-G, 2012).

Although institutions experience difficulties in providing an unlimited and reliable network, a number of schools have proved successful in this endeavor. Prince George's Community College (PGCC) of Maryland recently began implementing a wireless communications network on campus. The system offers unlimited wireless Internet access on campus via a variety of mobile devices through a secure connection (Violino, 2012). One advantage that PGCC now offers to students is connectivity anytime/anywhere on campus. "The College doesn't have to run cabling or dispatch network engineers to patch outlets. There's a significant savings at our remote centers because they are 90 percent wireless" (Violino, 2012).

Lansing Community College (LCC) in Michigan and Northern Virginia Community College (NVCC) are other great examples of schools that provide unlimited wireless access to their students across campus, with consistent upgrades and expansions of their capacity. LCC's chief information officer, Kevin Bubb, offered sound advice to colleges weighing the benefits of a BYOD program:

> The challenges of running a BYOD program are twofold: support and security. To what degree does the college provide support for personally owned devices? Do we support all devices, just a select few that we have experience with, or none at all? Take your time, BYOD is a complicated topic requiring a balance of access and security and a shift from the command and control approach IT has generally taken in the past. There are many issues and challenges that need to be researched, considered and addressed. (Violino, 2012)

Along the same line, NVCC encourages students to BYOD but does not have a dedicated program. Dean of learning and technology resources Frances Villagran-Glover admitted that in recent years a significant increase of students do BYOD, and the school's biggest challenge is providing the availability of access points to support the bandwidth capacity (Violino, 2012). Additionally, the school's IT department is in the process of

developing a student "sandbox" (Violino, 2012) program that gives students the opportunity to discover new ways to utilize mobile applications (Violino, 2012). Villagran-Glover stated:

> Fortunately, we have been able to meet this need through our campus (technology) funds. Wireless access points and charging stations are now part of our budget planning and new building projects. Because we all learn in different ways, we want students to customize their mobile devices and leverage their devices for (education). We think the opportunities are endless for both students and faculty. (Violino, 2012)

Fortunately, NPS is among the many schools that are extremely successful in providing uninterrupted Internet access. The school is well equipped to support its current capacity of students and faculty and falls within the 85 percent of colleges and universities that already provide a wireless network. Coverage at NPS includes not only all classrooms, offices, and the Dudley Knox library, but also most other campus hotspots where students congregated to study and socialize, such as the courtyards, lounges, and dining facilities. With the wireless connectivity being as robust as it is, hundreds of NPS users are seen daily taking advantage of the anytime/anywhere wireless network.

Another major reason for NPS's success in providing uninterrupted access is the fact that no students live on campus. At most colleges and universities that provide residency to students, IT departments observe an abundant amount of bandwidth usage after normal working hours. During this time, many of the intense bandwidth activities, such as gaming, video streaming, and social networking take place, causing significant setbacks in network speeds. However, at NPS, these types of activities are rare with students tending to vacate the premises after normal classroom hours. Furthermore, during schooling hours, students who are on campus but not attending lecture are often seen engaged in low-bandwidth usage activities, such as research or online testing.

Supporting the wide range of student and faculty bandwidth usage that derives from the BYOD program at many collegiate institutions requires significant network upgrades and better wireless access points to provide dense coverage throughout campuses. Institutions that are proactive in their response stand to gain many more critical benefits than those that do not. NPS is one of the many proactive schools that

have already implemented such resources and have proved successful in their efforts. Due to technologies in place, transition to a full BYOD program on campus, from a network perspective, would require minor capability upgrades.

3. Faculty Support

According to the *21st Century Campus Report*, the number one challenge campuses face in their efforts to increase classroom technology use by introducing a BYOD setting is the faculty's lack of technology knowledge (Ullman, 2013). Many campuses are currently working with the instructional leadership on altering the instruction in order to take advantage of new resources being introduced into today's teaching environments. However, even though 81 percent of colleges and universities are providing technology-specific professional development, faculty members express concern with the lack of common approaches, such as classroom seminars and group discussion (Ullman, 2013). Furthermore, instructors without the proper training and capability cannot train their students on the changes and upgrades to the use of technology, and professional development sessions would remain at the status quo. "If the professors and the instruction are not ready for BYOD, then it will not be successful. It is about creating student-centered instruction that allows students to use technology to its fullest" (Ullman, 2013).

Campuses' IT staff play a similar role, if not bigger, in regards to adjusting and conforming to the ample changes required for BYOD. BYOD and virtualization are similar concepts that allow anytime/anywhere computing via the Web. IT departments have the ability to support BYOD transformation and satisfy a wide range of computing needs of all students and staff by virtualizing servers, clients, application, and storage (Ullman, 2013). Users operating with older computing devices would still be able to keep up with those who utilize the latest equipment.

In 2011, Menlo College reported that its IT department made virtualized clients available to students enrolled in a financial accounting class (Ullman, 2013). Students were granted 24-7 access to online assignments and documents, which allowed them to work in specialized accounting software applications, store their in-progress projects, and

collaborate with other students. According to Ullman, “Virtualization also can help colleges and universities lower computing and labor costs, increase flexibility, improve security and reduce their carbon footprint” (2013).

IT departments for schools that do operate on a BYOD setting are less pressured to repair malfunctioning computing devices of their students. However, even though they are not responsible for conducting maintenance on the actual device, they are required to provide users with unlimited access to the network. This requirement often poses a problem because the IT staff must be familiar with the variety of operating systems utilized by both the faculty and students. Ullman states, “The best way to overcome this challenge is to develop written policies that specify which platforms the IT department will support” (2013).

4. Security Concerns

Security concerns are one of the most crucial topics when reconfiguring an installation’s computer system and data. A handful of colleges and universities have documented that BYOD security relates strongly to the end-node problem, wherein a device is used to access both sensitive and risky networks and services (Wiech, 2013). Because of Internet-based risks, some very risk-adverse organizations issue devices specifically for Internet use.

BYOD is known to cause data breaches, specifically among military schooling institutions that require students to access sensitive or classified information. Students who use a smartphone to access the school’s network have the potential to lose that phone, resulting in untrusted parties retrieving any unsecured data the phone retained. A challenging but important task for schooling institutions who utilize BYOD is to develop a policy that defines exactly what sensitive information needs to be protected and which students should have access to this information, and then to educate all students on this policy (Wiech, 2013). In addition to the personal security of students accessing and sharing information, personal devices carrying viruses that could possibly infect the entire internal campus resources of NPS is certainly the greatest security concern.

Colleges and universities with existing BYOD programs have been long adapting their networks and policies to accommodate the large number of security concerns that stem from personal mobile computing devices. Many of these institutions have established role-based authentication and virtual local area networks that prevent students from accessing internal applications, databases, and other sensitive or confidential data (Wiech, 2013).

The NPS IT staff should consider several different approaches to securing the network within a BYOD environment:

- Require users to register every device so that if a virus is introduced or a device attempts to access inappropriate areas, IT staff will have a way to tie devices to their users.
- Utilize two-factor authentication, in which both the user and the device are verified before network entry is allowed.
- Provide antivirus and antimalware software for all student, faculty, and staff computing devices.
- Scan devices at their points of entry to ensure they have virus protection and required patches.
- Educate students, faculty, and staff about security practices and network policies, as well as their own responsibilities as users, before network privileges are granted.
- Verify users' understanding of these practices and policies via signature or timestamp.
- Lock down the core network by adding additional firewalls around university financial systems and other mission critical applications or databases.
- Rely on virtualization and internal clouds to further protect financial and personal data. (Wiech, 2013)

With BYOD and cloud computing placing data at their users' fingertips, the concern of data breaches is huge when deploying these new mobile trends. Colleges and universities must understand this. In order to avoid an IT catastrophe, schools must recognize all the ways hackers could manipulate the system and cause a breach. It is highly recommended by several schools that have experienced the BYOD transition to call upon a trusted vendor to conduct the installation properly instead of trying to build the infrastructure from scratch (Wiech, 2013).

> In order to successfully defend against hacker attacks, colleges need to develop and maintain a well-rounded security infrastructure, ensuring that all endpoints are protected, to prevent infiltration into data centers, networks and databases. This is an intimidating task, but one that colleges will have to deal with in the foreseeable future. (Wiech, 2013)

Figure 11 shows the percentage of just how much hackers are responsible for all data breaches caused in 2012 and, more notable, the large percentage of how easy it is for the public to accidently cause a breach when a school is lax in creating their systems security domain (Daly, 2013b).

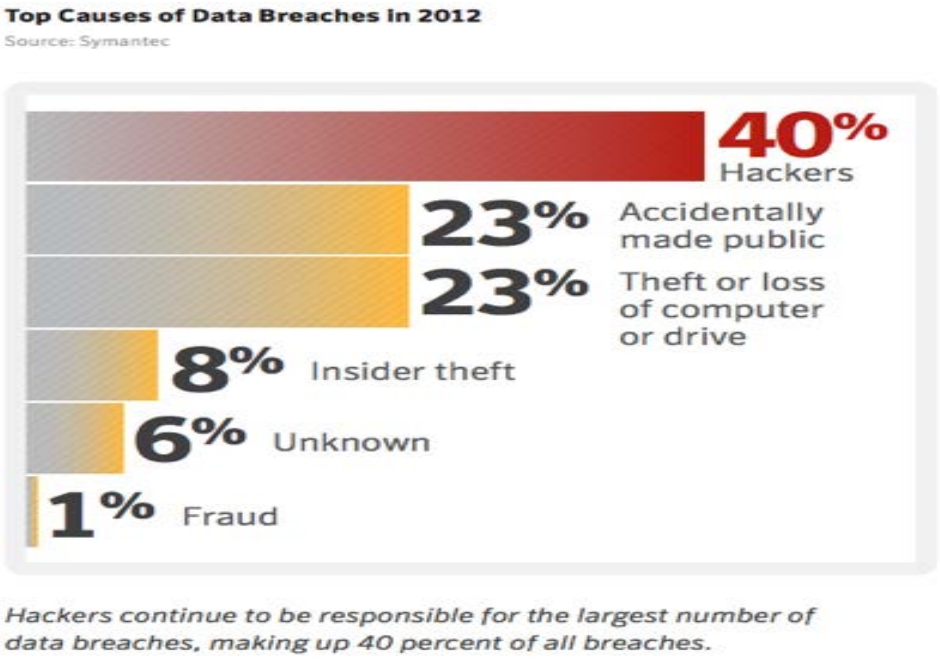

Figure 11. Leading Causes of Data Breaches (from Daly, 2013b)

III. METHODOLOGY

A. TECHNICAL ISSUES

To answer our thesis question on technical issues, we had to use an applied technique, meaning we had run a sample of application software used by the GSBPP that would be applicable to running in a BYOD environment under an application server. This required the assistance and support of the GSBPP's IT technician to install each software application on the server for further testing on the client devices. The software first needed to be installed on the application server for the testing on the application server. We found that when installed on the application server and run from desktop, some of the software had no technical issues in running.

We tested three applications of software: Oracle's Crystal Ball, StataCorps' Stata I/C, and Frontline's Risk Solver Platform. All three applications are statistically based simulation and optimization software used in various curricula in the GSBPP academic environment. The most important aspect of testing the software on the thin-client server was to ensure that the software could run flawlessly in such environment and ensure legal compliance with the software manufacturer EULA.

The technical specification for the GSBPP application server is as follows:

- Intel Core i7-3930K CPU @ 3.2GHz;
- Installed RAM: 64GB;
- 64-bit Operating System; Windows Server 2008 R2 Standard;
- Drive C: Samsung SSD 830, 512GB;
- Drive D: Western Digital WD2002FYPS-0, 2TB; and
- Drive E: Western Digital WD2002FYPS-0, 2TB.

STATA/IC is one of the programs we loaded onto 144 laptops to support GSBPP students. So we decided to use this as one of the test applications. Stata/IC is capable of working on a network utilizing the proper license. There was no retail packaging with the software because it was delivered via Internet download. The best way to check and ensure that the proper license is in possession would be either to check the electronic

purchase order or to call the company to confirm. Because we purchased the lab license, the software did not have any technical issues when running on the GSBPP application server.

Crystal Ball comes in Crystal Ball Classroom Faculty Edition, Crystal Ball Classroom Student Edition, Crystal Ball Decision Optimizer, and Oracle Crystal Ball Suite. The edition used by the GSBPP is the Crystal Ball Classroom Faculty Edition with a perpetual license. GSBPP acquired 35 licenses. Crystal Ball did not have any issues running in a thin-client environment, which made it useful in that students could work from home remotely if Crystal Ball was needed for any class homework assignments.

Frontline's Risk Solver Platform would not run in the thin-client environment. When the software is executed at the server's keyboard, it runs fine. When the software is executed remotely from a client-user machine, all of the program's functions are greyed out with no functionality on the user end. The company designed the software to disable execution when it is being run through a virtual machine interface, meaning it was engineered to be network aware and prevent execution from a client workstation. The Risk Solver (Frontline Solver, 2013) website indicates that the company offers a "flexible license" that would allow concurrent users. However, it is not apparent whether they offer it at the academic price. The commercial version of the software costs thousands of dollars per copy. But with each new faculty hire, there is a chance that GSBPP would need a different software package. In the current operating environment, this simply means that the GSBPP must buy a license for each government-owned laptop in use. However, because the license is tied to the machine, many users still benefit. So the answer in this case would be either to look at the "flexible license" as an alternative (if network accessible) or to find an alternative product that has the same benefits to the GSBPP academic environment, such as the free add-on version that comes with Microsoft Excel.

Alternatively, we also tried to see if MS Office 2010 would run out of the box; however, the standalone edition will not run on the thin-client because it refused to load on the application server. However, in further researching we discovered that Microsoft requires a specific version of Office 2010 to be loaded onto a server.

The whole point of testing applications or attempting to test applications on the application server lends both to understanding how software choices affects the choice to move to a BYOD environment and understand the legality of the software one is using or intending to use in such environment. The results of testing the software might mean having to compromise and using alternative software or upgrading the licenses. Whichever the case, understanding what the application server can and cannot do is just as important as understanding the costs.

B. COST ANALYSIS

Currently, the GSBPP maintains four smart classrooms comprised of approximately 144 government-procured laptops that are loaded with the software required for academic functions as dictated by the faculty. These laptops support a continuing enrollment of approximately 327 students.

Each of the laptops purchased by the GSBPP is maintained by two computer technicians at the GSBPP. The laptops are inspected, have any required adjustments made to the settings, have the required software installed, and are placed in the classrooms with a security tether to prevent loss. Each system is also inventoried and placed in the school's controlled equipage log, which is also maintained by the computer technicians.

The GSBPP is currently able to support no more than 32 classes whose instructors request a smart-classroom environment (four classrooms × four periods of instruction × two weekly offerings). This includes single courses that have multiple teachers and segments, such as the Introduction to Computer Systems Management Course, which has four class offerings in each semester of availability.

The GSBPP maintains a life-cycle replacement program that replaces between 32 and 72 government-owned laptops each fiscal year, depending on the size of the room being re-outfitted and the cost per laptop that meets specified contracting requirements. Essentially, one to two classrooms have their laptops replaced each fiscal year on a three-year cycle. Total budgeted replacement cost is $50,000 for the project, or about $1,000 to $1,600 per laptop for two years, and then $100,000 for the third year. If the money for

laptop replacement is budgeted early in the fiscal year, then a contract is put out for open bidding. If money is received later in the fiscal year, then the laptops are sourced through the General Services Administration (GSBPP Director of Instructional Technology, 2013).

The budget does not allow for hardware upgrades on existing laptops, and the construction of laptops in inventory would make upgrading nearly impossible. The school budgets for $10,000 for an annual replacement of an application server and also budgets for $10,000 each year for software purchases or upgrades (GSBPP Director of Instructional Technology, 2013).

For this section, we evaluated the costs associated with three courses of action (COAs) for the GSBPP to maintain the smart classrooms. Each of these COAs assumes the cost of employing support staff for GSBPP computers, the annual cost of completing a tech refresh on one of the smart classrooms, and the cost of software licensing.

1. Courses of Action

a. COA 1—Keep the Status Quo

In this section, we evaluate the full costs of maintaining the smart classrooms, fully staffing for support requirements, and completing a tech refresh for the laptops in at least one of the four classrooms per year, with two classrooms being refreshed in one year of the three-year refresh cycle. COA 1 establishes a baseline for comparing other possible COAs.

b. COA 2—Phase out the Current Smart-classroom System and Phase in a Full BYOC/BYOD Policy for the GSBPP

In this construct, no laptops would be replaced by the GSBPP when they are scheduled for a tech refresh.

c. COA 3—Partial Secession of the Smart Classroom Construct

The assumption is that not all students are going to have access to a computer capable of running the client software for an application server construct or that they may not be able to afford a laptop if one is not furnished for them through the U.S. military or their home country.

Currently in America, 82 percent of college students own their own laptops (Fottrell, 2013). We assume the numbers are higher for professional military officers who are graduate students attending classes, so we started with the assumption that holding seven laptops in each room, or 20 percent of the current number of computers in each smart classroom and 28 percent of average class enrollment for classes held in those rooms, would be sufficient for maintaining a learning environment for all students.

COA 3 creates a classroom environment where the majority of students will do schoolwork on their own device and will have the convenience of taking their work and their computer with them to easily save their files and continue their learning at another time or place. The minority of students who do not have devices capable of running the requisite programs will have access to the limited number of government-owned computers for in-class participation.

There are many ways to implement COA 3, but we concentrate on two possible means of implementation, from here on known as COA 3a and COA 3b. COA 3a assumes an annual tech refresh of a limited number of computers. The baseline for this figure is seven laptops per year or roughly 20 percent of the current annual purchase plan.

COA 3b assumes that no tech refreshes will occur while there are more operational computers owned by the GSBPP than what would be required for a limited smart-classroom construct. For example, 80 percent of all laptops would be removed from all four classrooms at the beginning of year one, and the oldest laptops, the ones due for a tech refresh in year one, would simply be replaced by the inventory from the classroom that had the most recent tech refresh.

To evaluate the cost associated with each of these student computing paradigms, we assume an average laptop purchase price of $1,300. This is the median price of recent contract purchases made by the GSBPP but is a solid working number that is supported by a continuing downward trend in laptop prices.

All data about the computer technician positions with the GSBPP are based on the statement of work used for advertising hiring for the position and in maintaining standards for worker responsibilities and performance. The cost for each employee hired as a computer technician is based on the current pay for a GS-7 step 5 employee (Office of Personnel Management, 2013).

We made certain assumptions about the number of computer technicians required to maintain the laptops in the smart classroom. The statement of work (SOW) sets the responsibility to operate and maintain instructional technology equipment at 25 percent of the total functions and responsibilities and sets maintain and process accountability records for controlled equipage at 20 percent. There are currently 144 laptops being maintained, and there are two full-time computer technician positions, each of which have 45 percent of their daily activities listed as maintaining the computers and the records pertaining to them. We therefore extrapolated that two full time computer technicians are theoretically required to maintain 64.8, rounded up to 65 laptops.

$$144 \times 0.45 = 64.8$$

Once the number of computers being maintained falls below 65, it may be feasible to replace one full-time position with a part-time worker. The part-time worker would concentrate on the initial installs of smart-classroom laptops and maintain the accountability records, thus freeing up the full-time worker to concentrate on the other 55 percent of responsibilities listed in the SOW as his or her full employment. If a construct were followed where the total number of computers maintained in the smart classrooms were reduced to zero, it may be feasible to employ only one full-time person in the position currently called *computer technician* and not have any part-time employees.

To compare the costs of each one of the COAs, we constructed a model that allows for controlling of such variables as the total number of computers maintained, the price of replacement computers, and the cost of software licenses that are installed on the application server.

Once the total number of computers being maintained in the model falls below 65, we assume that one of the computer technician positions could be vacated and the school would realize cost savings equivalent to the annual salary of the technician. Although this model leads to the conclusion that zero computers being supported would lead to zero employees being required, that is not the case due to the need to support other information technology in the classrooms and the portion of the SOW that calls for web building and technical support to faculty and students. Therefore, once the total number of computers being supported falls below 65, then we assume that a part-time employee is hired.

The model allows for an annual purchase of new laptops, based on the COA selected above, then adjusts inventory of computers being maintained, based on the carryover from the previous year, the number of laptops retired at the end of their life cycle, and the number of new computers purchased and placed into classrooms. Costs for the purchase price of the laptops, server support, and computer technician support are then calculated and the cost of smart-classroom operation is calculated.

The model specifically does not include the cost of infrastructure for supporting connectivity, such as Wi-Fi access ports and network servers. The network infrastructure for the GSBPP is already in place, and we do not anticipate additional costs for network support by replacing government-owned laptops with students' own devices.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS

A. SOFTWARE, LEGALITY AND SECURITY

Software makes up the most important aspect of utilizing a BYOD policy in the educational environment. BYOD use in education has been growing exponentially with more universities adopting the practice. However, the means of a secure communication solution is still needed for the efficiency of a BYOD program. Trends have focused on how to keep data safe and secure in the BYOD era. When shifting from a university-provided program where a computing device is provided by the university to a BYOD program, all software application, data, and communication resources are migrated to a thin-client server and not on a student's device. This also means that the IT department no longer has to worry about damaged, lost, or stolen computing devices that house its data.

With software comes the inequality of equipment being used by each student. When each student brings his or her own type of computing device, there is no longer a set device manufacturer with a clone of what software will run on each computing device. The IT department does not have the means to clone an individual's computing device, meaning that there will also be very limited technical support both in regards to hardware and the ability to run certain software off of the client-server. Certain software will require a minimum requirement to run, which may only run under a Windows operating system. Macintosh devices will vary in functionality, speeds, throughput, and performance when compared to a Windows-run device. The question will need to be answered regarding whether a Macintosh will have the same ease of functionality when running software from the client-server or connecting to the intranet via Virtual Private Network software utilized by the university. Therefore, the IT department, students, and faculty will experience inconsistencies in adapting to the BYOD environment. The current application software utilized by the GSBPP supports faculty and students in a variety of curriculums. Programs are installed on university-owned computing devices in classrooms and labs and are fully supported by the GSBPP IT department. All computers are Windows operating systems, so all patches, updates, virus-protection software, and all

functionalities of the computing devices are controlled to ensure strict adherence to security policies. The ability to ensure that the most up-to-date software is installed is paramount to security; however, when you go to a BYOD set-up, some of that functionality in ensuring compliance is lost. However, there is software that can be utilized to help mitigate such security concerns.

Universities use safe connect to enable access to its intranet or networks. NPS also utilizes safe connect, which is a network access control tool.

> SafeConnect [*sic*] is the most flexible network access control solution available and offers an easy to implement and support endpoint policy management system. It seamlessly connects into an existing multi-vendor network infrastructure while providing the flexibility to adhere to each organization's unique computing policy philosophies. SafeConnect's unique architecture provides a true out-of-line NAC solution that is vendor-independent, scalable, and flexible to meet your growth needs—resulting in reduced time, expense, and risk. (SafeConnect, 2013)

The SafeConnect software would be utilized by all students and/or persons accessing the NPS network while on/off campus, including both wired and wireless network connectivity. All users are then required to login to the SafeConnect webpage before they can access the campus network, especially content on the intranet page. The software wouldn't need to be installed on the client-server but on the individual users' computing device, supporting both Windows and Macintosh. All users would be required to download and install the SafeConnect Policy Key before accessing the network (see Figure 12).

> SafeConnect[*sic*] is used extensively by colleges, universities and K-12 school districts across the country. These environments are notorious for having large populations of unmanaged devices as well as significant security considerations. Industry analysts like Gartner and Frost & Sullivan identify Education as the proving ground for Network Access Control. (SafeConnect, 2013)

Figure 12. SafeConnect Install Screen (from SafeConnect, 2013)

Security is paramount whether operating in a BYOD environment or not. Software can easily be controlled and updated by the parameters set up by a university's security policy. Some of the top choices that universities and schools go with are McAfee: Total Protection; Symantec: Norton Antivirus; and SystemWorks: Norton Internet Security, just to name a few. However, there are few to no challenges when it comes to the IT department being able to implement, monitor, and update such software on school-provided computing devices. Most of these updates are done on a periodic basis and pushed by the IT department ensuring network compliancy. IT support changes when moving to a BYOD environment. Now this falls to the individual to keep his or her software up to date with the proper anti-virus or malware definitions installed.

SafeConnect will be able to interface with and recognize a variety of anti-virus software to verify that the anti-virus application is installed, updated, and operating properly. Although it is critical to have only one program, multiple programs can result in false-positive readings and prevent connection to the wireless network service, such as assessing the university's intranet. Individuals looking for free programs to run on their own computing device and ensure network connecting compliancy can use AVG or Avast! AV (free edition). Other well-known programs, such as Kapersky, McAfee, and Nod32 are also recognized and can be used. Because of the relative ease of installing SafeConnect and an anti-virus on an individual computer, lack of IT support does not create any challenges when transiting to a BYOD environment.

Software-management tools alone do not have the ability to address all security concerns. Sure, SafeConnect has the ability to check key elements, but it cannot address

anything like unlicensed software that the owner may have installed on his or her personal computing device, which could potentially compromise the integrity of the network. It also cannot address unsecured third-party connections, which most tablets have the ability to do in an unmonitored back channel. Infections by malware can also be an issues affecting user-owned computing devices. However, these are just some of the common findings that can arise when addressing issues of user-owned devices.

Licensing and intellectual property rights plays a big role in being able to successfully operate in a BYOD environment. Software management by the GSBPP IT department technicians have been paramount in ensuring that, if such implementation were to take place, they have met all legalities. GSBPP software applications are licensed under a variety of software propriety strategies, and under a sound management plan it has a detailed and comprehensive licensing plan that supports a per-user or per-device type of license, which allows a number of concurrent users. The GSBPP IT department has aimed to ensure strict compliance by procuring software that can legally and adequately run on the thin-client application server. However, challenges are still faced when either a new faculty or existing member wishes to use application software that may have not been properly tested or reviewed for legality of running on a thin-client server.

Every university has a different policy when it comes to software and how it is determined what can and cannot be used. If a university has a policy that says that the school will dictate what software applications are utilized in the classroom, then the challenges to support the end user greatly diminish. With a Department of Defense university, these policies are very different, especially when the university also hosts a variety of international students. Therefore, it is critically important that a policy be set forth to mitigate some of the challenges that are most common in the implementation of all BYOD environments. The biggest issue is being able to test the application on the thin-client server or ensuring that the proper license is offered to run in a network environment. The last thing anyone wants to do is breach the licensing terms of the software and its providers. Finding the licensing terms and rights for the software application will help the faculty understand the software limitations or any violations of

GSBPP policy. However, it is clear that faculty do not understand the parameters that it takes to run software on a thin-client server; thus, faculty and other need to be educated to ensure that proper software is chosen to fit the appropriate model. However, when no policy exists to restrict software choices, it then becomes incumbent through pressure on the IT department to find a way to get it to work, and this in and of itself can lead to legal issues.

There has to be an interface with the IT department and faculty to ensure that the best practice and solution is met to support all parties in a BYOD environment, including the students. A compromise when choosing the right software and acknowledging that there may be a better suited alternative or a free edition that facilitates learning just the same has to be realized. The legal bounds in regards to software applications are easy to cross; therefore, any unique challenges need to be addressed adequately and often.

> The unique needs of educational users present a number of challenges for IT professionals tasked with providing access to applications and content in a wide variety of formats. Perhaps the biggest of these challenges is the sheer magnitude of school IT departments' responsibilities. Schools tend to have very small IT staff, which are typically responsible for managing huge numbers of teacher and student user accounts as well as a seemingly endless array of computers, laptops, tablets, and other devices. Finding ways to ease the burden of user device management and maintenance along with IT resources is essential to ensuring that already overworked IT staff members are able to keep pace with the demands placed on them, and to provide students and staff with access to computing and learning resources from home, school, lab, library, or the field. (Ericom Software, 2012)

Remote access to the NPS network is imperative to the entire campus. Faculty, resident and non-resident students (distance learning), and staff require access to network resources both on and off campus. Because of that, NPS has a robust policy in place to ensure the safety of its network infrastructure. This policy addresses network services availability, firewall refinements, and a security protocols and posture.

> Security and privacy of data and the network are conventional areas of responsibility for a centralized IT department. In the last several years, much progress has been made in institutionalizing a formal security program. This process included the appointment of an Information Assurance Manager, creating and filling a Privacy Officer position,

> officially assigning network security staff to the Information Assurance arena, commissioning external audits to suggest improvements and to validate policies, and adopting enterprise-wide procedures and protocols. The mission of the Information Assurance Program is to ensure availability, integrity, authentication, confidentiality, and non-repudiation of data while in transit and while stored. Further development is expected in vulnerability patch management, secure configuration, security auditing, and intrusion detections and response capabilities. Some of the future challenges include addressing emergent malicious activity, better detection of network security behavioral anomalies, and increasing the security. (Naval Post Graduate School, 2009)

B. COST ANALYSIS

The cost-analysis models presented in Tables 1 through 5 demonstrate a six-year cycle, or two scheduled tech refreshes for each smart classroom. All of the numbers presented are calculated using the methods described in the methodology section. Year 0 is a current year baseline and starts under the status quo of computers maintained and operating staff regardless of the COA selected, as we expect that GSBPP, or any other organization, would not immediately abandon recently purchased computers and immediately reduce staffing. None of the numbers presented are adjusted for inflation, which allows all numbers to be evaluated on a constant dollar basis. Additionally, we recognize that not all factors could be anticipated and presented in these models, specifically with the potential additional computer technician and other technical assistance, with managing software licensing and providing technical support to faculty and students. We therefore consider these to be a best-case scenario presentation of anticipated budgets.

1. Course of Action 1

COA 1 shows 36 computers purchased in four years and 72 computers purchased in years 2 and 5. The staff position remains fully staffed with two computer technicians maintaining 144 computers during each year. The total cost of COA 1 over a six-year period is $1,118,976, with costs fluctuating between $170,896 and $217,696 per year. This cost sets the baseline for measuring potential cost savings of other COAs.

Year 0 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	36	$1,300		$46,800
Server				$10,000
Software Licesnes				$10,000
				$170,896

Year 1 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	36	$1,300		$46,800
Server				$10,000
Software Licesnes				$10,000
				$170,896

Year 2 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	72	$1,300		$93,600
Server				$10,000
Software Licesnes				$10,000
				$217,696

Year 3 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	36	$1,300		$46,800
Server				$10,000
Software Licesnes				$10,000
				$170,896

Year 4 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	36	$1,300		$46,800
Server				$10,000
Software Licesnes				$10,000
				$170,896

Year 5 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	72	$1,300		$93,600
Server				$10,000
Software Licesnes				$10,000
				$217,696

Total Costs	**$1.118.976**

Table 1. COA 1

Year 0 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$124,096

Year 1 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	3	36	108	
Limited Smart Classrooms	0	0	0	
Total Computers Maintained			108	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$124,096

Year 2 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	2	36	72	
Limited Smart Classrooms	0	0	0	
Total Computers Maintained			72	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$124,096

Year 3 costs				
Computer techs	1	$52,048		$52,048
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	0	0	0	
Total Computers Maintained			0	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$72,048

Year 4 costs				
Computer techs	1	$52,048		$52,048
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	0	0	0	
Total Computers Maintained			0	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$72,048

Year 5 costs				
Computer techs	1	$52,048		$52,048
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	0	0	0	
Total Computers Maintained			0	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$72,048

Total Costs	**$588,432**

Table 2. COA 2

2. Course of Action 2

COA 2 again begins with four smart classrooms with approximately 36 computers per classroom. Year 0 shows a cost of $124,096, and as no new computers are purchased, this cost is maintained through year 2. Costs drop at the year 3 point, as the entire student-use computer inventory is removed from circulation, allowing for one of the computer technician spots to be removed from the payroll. At this point, we are unable to determine whether this staff reduction is truly feasible. It may not be realistic if manpower demands are high for technical support on student devices or if software licensing are difficult to manage.

Total cost of maintaining servers, applications, and the dwindling laptop inventory would come out to $588,432 over the six-year period. COA 2 shows a cost savings of $88,424 per year when compared to the status quo.

If the current inventory of government-owned laptops were scrapped and the current smart-classroom paradigm were deconstructed, then one of the computer technician positions could also be immediately removed and total costs for servers, software licenses, and support would immediately fall to only $72,048 per year.

Year 0 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	7	$1,300		$9,100
Server				$10,000
Software Licesnes				$10,000
				$133,196

Year 1 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	3	36	108	
Limited Smart Classrooms	1	7	7	
Total Computers Maintained			115	
Computers purchased	7	$1,300		$9,100
Server				$10,000
Software Licesnes				$10,000
				$133,196

Year 2 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	2	36	72	
Limited Smart Classrooms	2	7	14	
Total Computers Maintained			86	
Computers purchased	14	$1,300		$18,200
Server				$10,000
Software Licesnes				$10,000
				$142,296

Year 3 costs				
Computer techs	1.5	$52,048		$78,072
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	4	7	28	
Total Computers Maintained			28	
Computers purchased	7	$1,300		$9,100
Server				$10,000
Software Licesnes				$10,000
				$107,172

Year 4 costs				
Computer techs	1.5	$52,048		$78,072
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	4	7	28	
Total Computers Maintained			28	
Computers purchased	7	$1,300		$9,100
Server				$10,000
Software Licesnes				$10,000
				$107,172

Year 5 costs				
Computer techs	1.5	$52,048		$78,072
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	4	7	28	
Total Computers Maintained			28	
Computers purchased	14	$1,300		$18,200
Server				$10,000
Software Licesnes				$10,000
				$116,272

Total Costs	**$739,304**

Table 3. COA 3A

3. Course of Action 3a

COA 3a depicts the costs associated with limited tech refreshes where each year only approximately 33 percent of the current laptop inventory scheduled for a tech refresh is replaced. GSBPP would therefore gradually transition away from the current smart-classroom construct and move to classrooms with limited availability of government-owned computers.

Under this COA, there is a three year tech refresh cycle. During the first two years of the cycle seven computers are purchased, and 14 computers are purchased in the

final year of the cycle. This COA continues with the current plan of having all government-owned computers for no longer than three years.

Cost savings are immediately realized as the capital outlay for new computers drops 80 percent from the status quo and continues to stay at 80 percent of current costs each following year.

Assuming the best-case scenario, one in which no additional workers are required for licensing management or technical-support–related issues, then labor costs decrease in year 3. This reduction is made possible as one of the computer tech positions is transitioned to part time and the salary for the second worker is reduced by 50 percent, a total 25 percent labor decrease. Total costs for COA 3a are $739,304, a savings of $63,278 per year over the status quo.

Year 0 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	4	36	144	
Limited Smart Classrooms	0	7	0	
Total Computers Maintained			144	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$124,096

Year 1 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	3	36	108	
Limited Smart Classrooms	1	7	7	
Total Computers Maintained			115	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$124,096

Year 2 costs				
Computer techs	2	$52,048		$104,096
Full Smart Classrooms	2	36	72	
Limited Smart Classrooms	2	7	14	
Total Computers Maintained			86	
Computers purchased	28	$1,300		$36,400
Server				$10,000
Software Licesnes				$10,000
				$160,496

Year 3 costs				
Computer techs	1.5	$52,048		$78,072
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	4	7	28	
Total Computers Maintained			28	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$98,072

Year 4 costs				
Computer techs	1.5	$52,048		$78,072
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	4	7	28	
Total Computers Maintained			28	
Computers purchased	0	$1,300		$0
Server				$10,000
Software Licesnes				$10,000
				$98,072

Year 5 costs				
Computer techs	1.5	$52,048		$78,072
Full Smart Classrooms	0	36	0	
Limited Smart Classrooms	4	7	28	
Total Computers Maintained			28	
Computers purchased	28	$1,300		$36,400
Server				$10,000
Software Licesnes				$10,000
				$134,472

Total Costs	**$739,304**

Table 4. COA 3B

4. Course of Action 3b

COA 3b, unsurprisingly, is very similar to COA 3a for total costs. The differences lie in how the smart classrooms are initially transitioned from having computers for all students to being 80 percent BYOD and 20 percent government-owned computers.

Due to the inventory of computers currently on hand, no new computers would necessarily need to be purchased in the first two years, but new computers would need to be purchased for all four smart classrooms in years 2 and 5. Staff cost reductions for COA 3b mirror COA 3a as the maintenance responsibilities and staffing requirements decrease at essentially the same pace for either COA.

Total costs for COA 3b over the six-year period would be $739,304. Again, this saves $63,278 per year over the status quo but does so with significantly higher budget fluctuations than COA 3a. If no staff positions can be eliminated, then the only cost-savings potential for any of the COAs would be the reduction in the budget for the purchase of new laptops.

5. Summary

The following table presents an overview of the distribution of total costs from year to year for each of the various COAs.

		COA 1	COA2	COA 3a	COA 3b
Year 0	Labor	$ 104,096.00	$ 104,096.00	$ 104,096.00	$ 104,096.00
	Hardware and Software	$ 66,800.00	$ 20,000.00	$ 29,100.00	$ 20,000.00
	Total	$ 170,896.00	$ 124,096.00	$ 133,196.00	$ 124,096.00
Year 1	Labor	$ 104,096.00	$ 104,096.00	$ 104,096.00	$ 104,096.00
	Hardware and Software	$ 66,800.00	$ 20,000.00	$ 29,100.00	$ 20,000.00
	Total	$ 170,896.00	$ 124,096.00	$ 133,196.00	$ 124,096.00
Year 2	Labor	$ 104,096.00	$ 104,096.00	$ 104,096.00	$ 104,096.00
	Hardware and Software	$ 113,600.00	$ 20,000.00	$ 38,200.00	$ 56,400.00
	Total	$ 217,696.00	$ 124,096.00	$ 142,296.00	$ 160,496.00
Year 3	Labor	$ 104,096.00	$ 52,048.00	$ 78,072.00	$ 78,072.00
	Hardware and Software	$ 66,800.00	$ 20,000.00	$ 29,100.00	$ 20,000.00
	Total	$ 170,896.00	$ 72,048.00	$ 107,172.00	$ 98,072.00
Year 4	Labor	$ 104,096.00	$ 52,048.00	$ 78,072.00	$ 78,072.00
	Hardware and Software	$ 66,800.00	$ 20,000.00	$ 29,100.00	$ 20,000.00
	Total	$ 170,896.00	$ 72,048.00	$ 107,172.00	$ 98,072.00
Year 5	Labor	$ 104,096.00	$ 52,048.00	$ 78,072.00	$ 78,072.00
	Hardware and Software	$ 113,600.00	$ 20,000.00	$ 38,200.00	$ 56,400.00
	Total	$ 217,696.00	$ 72,048.00	$ 116,272.00	$ 134,472.00
Total		$ 2,133,856.00	$ 1,072,768.00	$ 1,374,512.00	$ 1,374,512.00

Table 5. COA Summary

C. LESSONS LEARNED

1. Student IT Agenda

With the wide range of available computing devices sold in today's IT market, the numerous advantages of shifting to a BYOD program has obvious appeal. With that said, once it is time for students to purchase their devices, which should they choose? Often, rather than basing their decision on enhancing their educational values, college students tend to derive their choice from the latest trend, fashion, or even what they can best afford. This is where the college and university staff must agree on the significant pedagogical implications that each device has.

In a BYOD environment, faculty must cater to the least powerful computing device in the classroom. The least expensive devices are typically designed for consumption versus creation. Given that creation is still possible, it is often minimal among cheaper devices and is therefore more difficult to keep up with classmates. Understanding and outlining these potential setbacks and "discussing the pedagogical objectives of school computing with all of the teaching staff" (Tierney, 2011) before implementing a BYOD program is key. Figure 13 is a handy reference that displays the capabilities offered by some of the more popular devices available today.

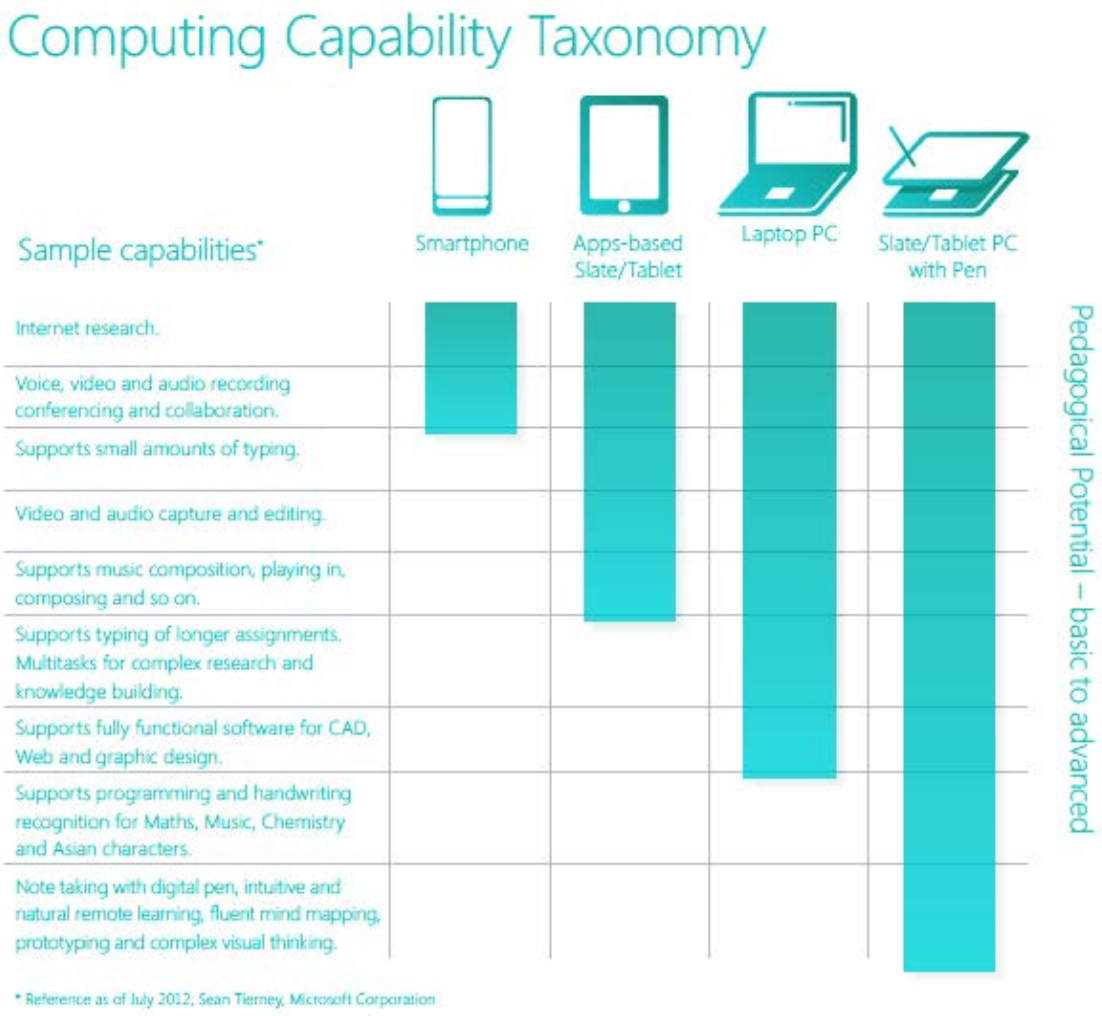

Figure 13. Bring-Your-Own-Device Computing Capabilities (fromTierney, 2011)

Smartphones, Apps-based slate/tablets, laptop PCs, and slate/tablet PCs with pen are the four most used computing devices around college and university campuses today. Each device offers unique capabilities; however, in terms of pedagogical potential, some are far more advanced than others.

The majority of college students nowadays have a smartphone and often uses it to support some aspects of the learning experience. Although fairly limited, students can conduct online research via Internet connection and access university administration devices. A great example of this at NPS is students' ability to access Sakai and conduct daily muster via their phone. Other capabilities are the phones' basic programs, such as video, camera, and voice recordings, which can all be used to record student lectures and presentations. Furthermore, latest technologies continue to develop new educational applications and electronic books accessible via smartphone (Tierney, 2011).

An apps-based slate/tablet offers all of the same educational services and more at a slight increase in cost. In addition to a larger screen, making it easier to write and read, slates and tablets include digital keyboards. Digital keyboard allow students to take notes and create opportunities for content making. Although light in weight, apps-based slates/tablets do not contain the processing power nor the compatibility to maintain the latest educational applications (Tierney, 2011).

Laptop PCs are generally the most common device found amongst college students these days. With all of the educational capabilities of a smartphone and apps-based slate/tablet, laptop PCs offer the use of a full keyboard. This is a significant advantage, especially for students in our current generation who have excelled in typing throughout their path of education. This allows for quick online research and swift note taking ability. Additionally, laptops provide increased performance levels that allow them to run advanced educational applications, including music, graphics, and specific curriculum based programs (Tierney, 2011).

As seen in Figure 17, the slate/tablet with pen is the device with the greatest pedagogical potential in today's schooling environment. Equipped with all of the learning capabilities of the previous three items mentioned, the slate/tablet with pen are designed

for a full learning experience. The biggest advantage is that this item contains a digital pen for handwriting. The digital writing allows students to take down notes but then convert them to an organized text. Also, these items can operate in various languages. According to Tierney, “Schools will have to consider carefully the purposes to which the devices are to be put to when developing their own BYOD policies” (2011).

2. Supporting Network

As discussed in our literature review, NPS has one of the best supporting networks a college or university has to offer. The IT faculty and staff are dedicated to ensuring that their students receive the state-of-the-art technologies, networking abilities, and developments to support the schools extensive research. A member of the Corporation for Educational Network Initiatives in California (CENIC), NPS works closely with higher education research organizations across the country as a connector with Internet2 and global networks. Recently, the school upgraded its network to a high tech 10G+ optical system and is on track for multiple 10G connections to CENIC along with other network providers. This type of network infrastructure is ideal for a BYOD implementation as it includes the following capabilities:

- cloud computing architectures,
- unique file system,
- high speed transport protocol technologies,
- high performance computing clusters and distributed grid computing,
- virtualization,
- advanced network security applications,
- next generation optics and control planes, and
- network visualization tools for high bandwidth applications.

These system enhancements, coupled with the familiarity and comfortableness students obtain by utilizing a computing device of their choice, would likely increase breakthrough research activities conducted by both students and staff. According to NPS Public Affairs Officer, “This core infrastructure will be ready for 100G network applications in the years ahead, set by the solid network infrastructure today” (2013). Figure 18 illustrates the different levels of network development and evolution for the

California research and education community. NPS currently operates as a high performance research network, and given its leading-edge services for a large quantity of application users, its network technology resides at CalREN-HPR Tier 2.

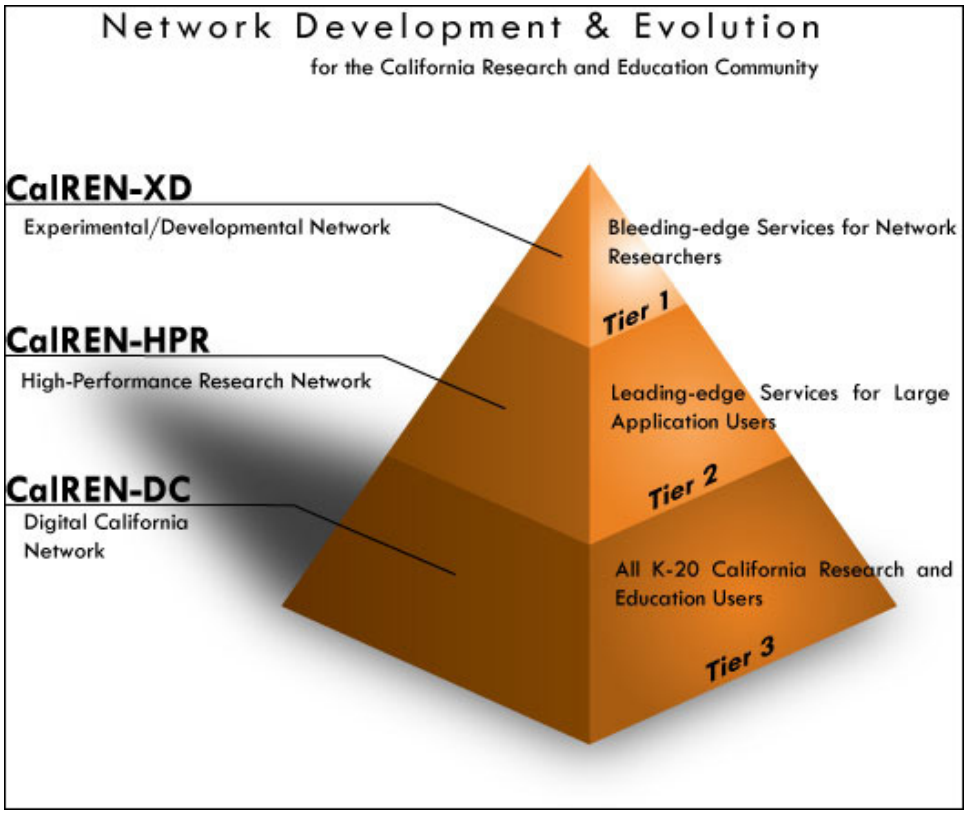

Figure 14. Network Development and Education for the California Research and Education Community (from NPS Public Affairs Officer, 2013)

3. Faculty

Our research has shown that there are two approaches to faculty concerns, one where the faculty must conform their instruction to be workable on the lowest-common-denominator equipment, and one in which the students are required to bring a device capable of running the requisite software for a class or laboratory work.

4. Student Responsibility

Under the paradigm where the students are responsible for bringing equipment, professors do not have to conform to the student's needs but rather can concentrate on

providing what they consider the ideal learning environment and can ensure that all students who do conform to requirements have the same learning experience. In this paradigm, students are required to adapt to classroom settings; if the instructor chooses to teach a course or assign projects using a specific computer program, then students are required to access that program via their own personal device.

As students are made responsible for ensuring that their laptops are capable of meeting their instructor's expectations, the demand for quality help desk support from the IT staff increases. The staff must be able to conduct support on many different versions of various operating systems and must understand the intricacies how the thin-client and individual applications will perform with high numbers of variables across multiple computing platforms. The students are still, of course, responsible for the physical hardware maintenance and may even find themselves in situations where they are required to make further investments in technology to remain enrolled in a class.

5. Lowest Common Denominator

Some institutions stated that their faculty had issues with conforming to the changes and challenges of BYOD. When faculty members are forced to adopt their methodology to conform to students' computers, then they must learn and be familiar with the least performing device in the classroom. This leads to a situation where instructors cannot necessarily teach their course the way they want to due to some student devices lack of program capability. The lowest-common-denominator paradigm does have the benefit of proving to be less stressing for IT staff resources as minimal software support required or reasonably expected.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

A. CONCLUSIONS

1. Technical Issues

We set out to determine whether all of the software used in the GSBPP curricula is compatible with a client–server architecture and whether the campus network infrastructure was reliable enough to support client–server architecture. During our research, we discovered that the technical issues are broader and more diverse than we anticipated and require substantial manpower and technical expertise to manage.

With solid infrastructure, software management, and security policy in place, the GSBPP can ensure that a BYOD environment supports the needs of the faculty, students, and staff. However, it will take a notable plan to ensure that such implementation can support international students and the challenges that individual users will face in the process. In a de-centralized IT infrastructure, it will be incumbent on the end-users to understand limitations of support when using their own computing device.

2. Cost Analysis

Upon first analysis of the research questions, we assumed that the current GSBPP setup of network capability and government-owned laptops provided the ideal situation for saving government funds by ceasing, or dramatically reducing, the purchase of additional computers each year for technical refreshes, and that labor costs could be similarly reduced.

Through the research process, we discovered that, due to other assigned responsibilities contained in the SOW, labor requirements, and therefore labor costs, would not fall as quickly as initially anticipated. Upon further research, we discovered that there is a potential that labor costs could actually maintain at current levels or even increase depending on the complexity of managing the thin-server architecture and software licensing complexities.

The best-case scenario analysis of COA 3 (a or b) presents an 80 percent reduction in laptop purchase requirements, but only a 25 percent decrease in labor costs. These savings combine for a total savings of $63,278 per year from the current paradigm.

3. Legal Issues

Our original research question was "Do all of the GSBPP software licenses permit operation under client–server architecture?" But we discovered that the legal issues should be viewed from a broader perspective.

All software currently used by GSBPP faculty in the classroom setting is allowable under the EULAs in place, and GSBPP does own the requisite licenses for legal operation; however, we discovered that this may not always be the case. Not all software allows itself to be installed under a server–client or thin-client architecture, and other software may come with legal restrictions that would make it impossible to operate under a BYOD construct.

4. Lessons Learned

Again, we set out to determine how GSBPP could apply lessons learned from other educational institutions in the implementation of a BYOD policy, but we found that a broader approach was warranted.

Few educational institutions are in a position where a full implementation of BYOD is a viable option at this time, but partial BYOD is growing a strong foothold in education, and a full implementation of BYOD is becoming the standard in many commercial ventures.

B. RECOMMENDATIONS

We recommend that GSBPP does not implement a BYOD policy at this time. Our research has demonstrated that cost savings may materialize, but we do not fully know to what extent they may present themselves. In addition, we believe that COA 2 would not be feasible in the current GSBPP environment due to a realistic scenario where

students either do not have the financial means to purchase a laptop, or they purchase a machine that is not fully compatible with the thin-client architecture or specific pieces of software.

The cost benefit to the school of going with either COA 3a or COA 3b would be no more than $63,278 per year under best-case scenarios, and we do not believe that the labor cost savings factored into that figure would be fully realized due to expected increased labor requirements for managing the complexities for staying compliant with legal requirements. Additional labor requirements will stem from managing new software installs and providing help desk support to both students and faculty to regulate a classroom environment conducive to electronic learning or the use of interactive software for instruction.

C. LIMITATIONS OF STUDY

In this section, we present a consolidated listing of the assumptions made in conducting this study and presents the limitations we faced.

1. Assumptions

The following assumptions were made in this study:

- Pay increases for GSBPP employees and budget increases for purchasing laptops, servers, and software would increase at the rate of overall inflation, and, therefore, there would be no requirement to consider the time value of money in considering the COA to recommend.
- The GSBPP network is fully capable of transitioning to a full or partial BYOD with no measurable change in service or reliability to the students and faculty.
- The GSBPP network would be maintained by a non-GSBPP budget indefinitely, regardless of the COA undertaken.
- A thin-client architecture can be operated at a negligible cost that fits within the current server and software licensing budget without impact to other services.

2. Limitations

We recognize the following limitations to our study and analysis:

- We are unable to test all software applications that may be deemed required for current or future courses of study.
- No survey(s) were conducted to capture the sentiments of GSBPP students and faculty on transitioning to a BYOD program.
- We are unable to fully monetize or capture the effects of a BYOD policy on international students who are unique to the GSBPP.

D. AREAS FOR FURTHER STUDY

Although we do not believe that implementing a full or limited BYOD policy is the correct move for GSBPP at this time in the current environment, we recognize that it may be the correct move for other educational institutions at this time and that advances in technology may soon make BYOD a better option for GSBPP and NPS. We recommend the following areas for further study in BYOD at institutions that do implement a BYOD policy.

- Do savings realized from discontinuing computer hardware purchases outweigh additional outlays in network infrastructure, servers, licensing, and salaries of tech professionals?
- Is there a demonstrable difference in the learning or test performance of students who use their own devices in comparison to students using school-owned computers in the traditional setting?

APPENDIX ABOUT THE AUTHORS

Lieutenant (LT) Jeff Carideo, originally from Holliston, Massachusetts, joined the Navy through the NROTC program while attending the University of Maine at Orono. In 2004, he graduated earning his bachelor's degree in business administration with a concentration in management and was immediately commissioned as a Naval Supply Corps officer. His first assignment upon graduating from the Navy Supply Corps School in Athens, Georgia, was aboard *U.S.S. Emory S. Land* (AS-39). Stationed in La Maddalena Italy, he served as the ships Disbursing/Wardroom Officer from December 2004 to Dec 2006 earning his Surface Warfare Supply Corps officer qualification. Immediately upon receiving orders to FISC DET NAS Jacksonville in January 2007, LT Carideo volunteered for a 15 month individual augmentation (IA) to Afghanistan. He was assigned to the 207th Army Corps and stationed at Camp Stone in Herat where he served as the Senior Supply Officer in charge of mentoring an Afghanistan National Army supply colonel of the Kabul Military Training Facility detachment. In April 2008, LT Carideo returned from his IA to begin his duties at the FISC DET NAS Jacksonville as the Material/Control Division Officer. During this tour he has completed the Joint Aviation Supply and Maintenance Material Management (JASMMM) course and subsequently earned his Naval Aviation Supply officer qualification. Remaining in the Jacksonville area, LT Carideo received orders out of Mayport in July 2010 serving onboard the *U.S.S. Boone* (FFG-28) as the ships supply officer. Upon returning from the ships final Southern Seas Deployment, he completed his department head tour by decommissioning the frigate in February 2012. At the Naval Postgraduate School, Lieutenant Carideo is completing an MBA degree in acquisitions and contract management. He has a follow-on assignment to the Logistics Support Unit in Little Creek, Virginia.

Lieutenant (LT) Timothy Walker is a native of Caledonia, Ohio. He graduated from Maranatha Baptist Bible College in 2003 and was commissioned through Officer Candidate School in 2004. Upon completion of the Basic Qualification Course at Navy Supply Corps School, LT Walker reported to NMCB 74 in Gulfport, Mississippi where

he served as disbursing officer and food service officer. He also served as logistics coordinator and transportation officer during field exercises and mount out operations. LT Walker's second operational tour was as the supply officer for EODMU 11 on Whidbey Island, WA, with whom he forward deployed to Kandahar Afghanistan as the CJTF-4 for CJTF Paladin South Counter-IED. Upon return to CONUS, he coordinated the transportation and logistics of moving all command material for a homeport shift to Imperial Beach, California (CA). After his department head tour, LT Walker reported to CTF 53 in Manama, Bahrain, where he served as the air routing officer. He was responsible for coordinating all fixed wing and rotary logistics movements for NAVCENT, conducting both crisis and deliberate logistics planning for Joint Exercises and Humanitarian Aid and Disaster Relief throughout the AOR. LT Walker is currently a student in the Financial Management Program at Naval Post Graduate School where he will graduate with an MBA and complete JPME Phase I in December 2013. LT Walker resides in Monterey, CA with his wife, Page, and two young children.

Lieutenant (LT) Jason Williams is a native of southern California. He is a 2003 graduate of the California Maritime Academy (Cal Maritime) where he graduated with a Bachelors of Science in Logistics and International Transportation; completing an international training cruise to South America onboard the training ship *Golden Bear* in 2000. In 2002, he enlisted in the inactive Naval Reserves delayed entry program and received his commission through the Naval Officer Candidate School; Pensacola Florida in 2003. LT Williams's initial sea tour was onboard USNS Saturn (T-AFS 10) as material officer and assistant stock control/administration officer. His shore assignment was supply officer; Joint Maritime Facility, St. Mawgan United Kingdom. Dual hatted, he served as regional supply officer; Fleet Industrial Supply Center, Sigonella, supporting the Southwest region of the United Kingdom. His later sea duty assignment(s) include supply officer onboard the *U.S.S. Ponce* (LPD-15). LT Williams is currently earning a master's degree in supply chain management from Naval Postgraduate School Graduate School of Business & Public Policy.

LIST OF REFERENCES

Admin. (2013, March 7). Get to know the two major groups of computer software [Web log post]. Retrieved from http://www.cloudcamb.org/around-the-world/get-to-know-the-two-major-groups-of-computer-software

Ardoin, P. (2010, March). Is your enterprise ready to “bring your own computer?” Retrieved from www.visionapp.com

Baker, K. (2012, November 6). How to prevent license overkill from stifling the BYOD revolution [Web log post]. Retrieved from http://www.techrepublic.com/blog/tech-decision-maker/how-to-prevent-license-overkill-from-stifling-the-byod-revolution/

Brandell, M. (2012). BYOD: Where the costs are. Retrieved from http://www.networkworld.com/news/2012/110612-byod-264002.html

Bring your own device to work: Is BYOD a problem for small business? (2012). *Smart Computing*, 45–46. Retrieved from http://www.smartcomputing.com/DigitalReader/Default.aspx?IssueName=SC___2310__#45

CDW-G. (2012). Bring your own device. *Ed Tech*. Retrieved from http://www.edtechmagazine.com/higher/sites/edtechmagazine.com.higher/files/108532-wp-hied-byod-df.pdf

Chao, K (2010, August 19). Software categories [Diagram]. *Wikimedia Commons*. Retrieved from http://commons.wikimedia.org/wiki/File:Software_Categories.png

Cohen, D. (2011, November 15). What is an EULA? Retrieved from http://what-is-what.com/what_is/eula.html

Computing Tech. (2011, November 16). Cloud versus client-server [Web log post]. Retrieved from http://computingtech.blogspot.com/2011/11/cloud-versus-client-server.html

Daly, J. (2013a, June 4). Why higher education is the target of hackers, phishers and spammers. *Ed Tech*. Retrieved from www.edtechmagazine.com/higher/article/2013/06/why-higher-education-target-hackers-phishers-and-spammers

Daly, J. (2013b, June 5). These 14 BYOD statistics tell a story of opportunity and danger. *Ed Tech*. Retrieved from http://www.edtechmagazine.com/higher/article/2013/06/these-14-byod-statistics-tell-story-opportunity-and-danger

DevTools. (2011–2012). *SoftwareLicensing.* Bangalore, India: DevTool.

Distributed Management Task Force. (2011, February 28). DMTF to examine need for software license management standards. Retrieved from http://www.dmtf.org/news/pr/2011/2/dmtf-examine-need-software-license-management-standards

Ericom Software. (2012). Chromebooks and BYOD success in educatio*n.* Retrieved from http://www.ericom.com/specs/WP-Chromebook-and-BYOD-Success-Education.pdf

Fottrell, Q. (2013, July 31). PCs outsell tablets in college dorms. Retrieved from http://www.marketwatch.com/story/pcs-outsell-tablets-in-college-dorms-2013-07-30

Frontline Solvers. (2013). Frontline systems software license. Retrieved from http://www.solver.com/license

Gabrial, T. (2010, November 4). Learning in dorm, because class is on the Web. *New York Times*. Retrieved from http://www.nytimes.com/2010/11/05/us/05college.html?pagewanted=all&_r=2&

Gartner. (2011, October 17). Gartner says worldwide enterprise IT spending to reach $2.7 trillion in 2012. Retrieved from http://www.gartner.com/newsroom/id/1824919

Golftheman. (2012, December 10). Operating system placement [Diagram]. *Wikimedia Commons*. Retrieved June 5, 2013, from http://commons.wikimedia.org/wiki/File:Operating_system_placement.svg

GurockSoftware. (2011). Selecting the right license strategy for your software [Web log post]. Retrieved from http://blog.gurock.com/articles/selecting-the-right-license-strategy-for-your-software/#conclusion

Kabak, M. (2013, March). Enforcement of end-user license agreements for California software developers [Web log post]. Retrieved from http://www.sanfranciscobusinesslawyerblog.com/2013/03/enforcement-of-end-user-license-agreements-for-california-software-developers.html

Kelsey, J. (2012). Going virtual? Stay true to licensing rules. Retrieved from http://www.expressmetrix.com/products/software-license-management/

Kolowich, S. (2010, January 5). Serving the laptopless student. Retrieved from http://www.insidehighered.com/news/2010/01/05/labs#ixzz2dD7tqOLk

Microsoft. (2013). Volume licensing. Retrieved from http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx

Myer, B. E. (2013, January 28). Thin client model and BYOD [Web log post]. Retrieved from http://www.vmblog.com/archive/2013/01/28/thin-client-model-and-byod.aspx#.UH0mN2RK7B8

Myers, J. (2012, September 7). Software licensing and BYOD [Web log post]. Retrieved from http://en.community.dell.com/dell-blogs/software/b/software/archive/2012/09/07/software-licensing-and-byod.aspx

Naval Postgraduate School. (2009). *IT Strategic Plan 2009.* Retrieved from http://www.nps.edu/Technology/Documents/NPS%20IT_Strategic_Plan%20June%202009.pdf.

Naval Postgraduate School Public Affairs Officer. (2013). Naval Postgraduate School networks. Retrieved from http://www.nps.edu/Technology/Documents/NPS%20Network.pdf

Office of Personnel Management. (2013, January). Salary table of 2013-SF incorporating locality payment of 35.15%. Retrieved from http://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2013/general-schedule/sf.pdf

Oracle. (2013). Oracle Crystal Ball classroom edition. Retrieved from http://www.oracle.com/technetwork/middleware/crystalball/overview/index.html

SafeConnect. (2013, September 20). SafeConnect network access control. Retrieved from http://www.impulse.com/higher-education/

Stata. (2013). End-user license agreement (EULA). Retrieved from http://www.stata.com/order/end-user-license-agreement/

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management*, *30*(2), 109–116.

Sweeney, J. (2012). *BYOD in education*. Retrieved from http://i.dell.com/sites/doccontent/business/solutions/brochures/en/Documents/2012-nine-conversations-byod-education_au.pdf

Tierney, S. (2011). Bring your own device to school. Retrieved from http://download.microsoft.com/documents/Australia/EDUCATION/2012008/Bring_your_own_device_to_school_briefing_paper_K-12.pdf

Twentyman, J. (2012, September 3). BYOD: OMG! or A-OK? *SC Magazine*. Retrieved from http://www.scmagazineuk.com/bring-your-own-device-omg-or-a-ok/article/258449/

Ullman, E. (2013, February 5). BYOD: One year later. Retrieved from http://www.techlearning.com/features/0039/all-play-and-no-work/53433

Violino, B. (2012, August 21). BYOD: Bring your own device to campus. *Community College Times*. Retrieved from www.communitycollegetimes.com/pages/technology/BYOD-Bring-your-own-devices-to-campus.aspx

Wiech, D. (2013, January 28). The benefits and risks of BYOD. Retrieved from www.mbtmag.com/articles/2013/01/benefits-and-risks-byod

Winkelman, R. D. (2013). An educator's guide to school networks. Retrieved from http://fcit.usf.edu/network/chap6/chap6.htm

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California